La ley de reciprocidad cuadrática y sus generalizaciones

Sara Embid Solano

Trabajo de fin de grado en Matemáticas
Universidad de Zaragoza

Director del trabajo: Fernando Montaner Frutos
Directora del trabajo: Paz Jiménez Seral
11 de septiembre de 2020

Agradecimientos

Gracias a dos de tantas profesoras de matemáticas de instituto por las que profesé una simpatía especial. A la primera de ellas, por mostrarme un día cualquiera la definición formal de límite y hacerme ver que las matemáticas requieren rigor. A la segunda, por mostrarme la parte lúdica y permitirme diseñar una ecuación cuadrática que tuviese como solución la nomenclatura asignada a nuestra clase que, si bien, no es ningún logro, me permitió conectar con una calidez inusual en los procesos matemáticos.

Gracias al personal de los talleres de talento matemático en los que participé antes de matricularme en la universidad así como al personal de la semana de inmersión en matemáticas. Recuerdo con especial cariño e ilusión la primera vez que me mostraron las congruencias y pude trabajar con ellas.

Asimismo, gracias a los profesores del departamento de álgebra que se han ido y a los que todavía continúan. A Pilar por iniciarnos en el álgebra lineal y meternos en la cabeza que "uno debe saber siempre dónde está". También a Vicente, por ese carácter afable y esa pasión, nada contenida, hacia los números, como bien él decía "los números son maravillosos".

A mis directores Paz y Fernando, que comparten también esa serenidad y ese gusto por unas matemáticas que se construyen y nos revelan conexiones inusuales. Por ese entusiamo contagioso y esa apreciación de la belleza, gracias.

A mis compañeros de carrera que me tienen como referente para determinar si un número es bonito o no y escuchan con delicado mimo mis desvaríos. A Alma, a Alba, a Cristina, a Cecilia, a Mireia, a Juan Carlos, a Roberto, a Juan, gracias. Mención especial tiene Juan, por apoyarme incondicionalmente y ver en mi cualidades deseables para ser una buena matemática.

Por supuesto, agradecer a mi familia, la que me viene dada y a la que elijo conscientemente para formar parte de mi vida. También a toda persona a la que le hablo de números primos y me escucha. En estos tiempos y siempre, es necesario que haya oídos dispuestos a atender conversaciones de esa índole.

Enormemente agradecida a todos.

Prólogo

La motivación del presente documento reside en dar luz a la ley de reciprocidad cuadrática, también conocida como “aureum theorema" o teorema áureo por Gauss. Esta ley se presenta como uno de los objetos de estudio clásicos de la teoría de números. Ahora bien, si pretendemos acudir a su génesis, tenemos que remontarnos antes a Bachet con su traducción del griego al latín de la Arithmetica de Diofanto (1621). En el problema 9 del libro V de dicha colección ya se pone de manifiesto que ningún número de la forma $4a-1$, o lo que es lo mismo, $4a+3$, puede ponerse como suma de dos cuadrados. Cuestiones asociadas a las leyes de reciprocidad fueron tratadas por matemáticos de renombre: Fermat, Euler, Legendre, Lagrange y Gauss, entre otros. De hecho, se piensa que el teorema áureo fue descubierto independientemente por Euler, Legendre y Gauss. En la actualidad se han dado más de 240 demostraciones distintas, algunas fruto de aportaciones ingeniosas a demostraciones previas.

Este trabajo no pretende más que un acercamiento tímido a semejante resultado. Los tres capítulos de los que dispone no son más que una selección gradual de los procesos de abstracción en la mente de un matemático. Se parte de un espacio aparentemente compartido por todos, el de los números enteros y se recorren después “enteros” más especiales como son los enteros gaussianos y ya de modo más general, los enteros cuadráticos que engloban a estos últimos. Aunque el lector necesitará familiarizarse con ciertos conceptos previos - vitales para la comprensión de la ley - damos aquí los distintos enunciados que presenta en dos espacios claramente diferenciados.

- Sean $p,q \in \mathbb{Z}$ dos primos impares distintos, entonces $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{4}(p-1)(q-1)}$.
- Sean $\lambda,\ \mu \in \mathbb{Z}[i]$ dos primos gaussianos impares y distintos, entonces $\left[\frac{\lambda}{\mu}\right] = \left[\frac{\mu}{\lambda}\right]$.

Solamente nos atreveremos a demostrar la ley descrita en $\mathbb{Z}$ y aunque en el anexo, uno puede encontrar una demostración que se apoya en contar los puntos que satisfacen una determinada propiedad, la preferida por el autor e incluida en el cuerpo del trabajo será una de tantas que nació del ingenio de Gauss. Más concretamente, la sexta prueba, aquella que utiliza lo que se conoce como sumas de Gauss, que no es otra cosa que sumas de raíces primitivas de la unidad. Para conocer todos los detalles relativos a la versión para $\mathbb{Z}[i]$, viene bien tener a mano [1].

Ya Gauss mostró que ciertos números irracionales proporcionaban información útil sobre los enteros. Si se tiene en mente la apariencia de $\mathbb{Z}[i]$, uno reconoce a sus elementos por ser aquellos números complejos restringidos a tener parte real y parte imaginaria entera. En este anillo, la ley se presenta con una expresión más simple. Conociendo que esa notación extraña $\left[\frac{\lambda}{\mu}\right]$ sirve para denotar si un número es o no un resto cuadrático en $\mathbb{Z}[i]$ o dicho de otro modo, denotar si existe o no un elemento $\nu \in \mathbb{Z}[i]$ t.q. $\nu^2 \equiv \lambda \pmod{\mu}$, la ley afirma que si dicho cuadrado existe para λ también lo hará para μ (y viceversa). Lo mismo para el caso en que uno no sea resto cuadrático, el otro tampoco lo será.

Los restos cuadráticos se utilizan para hacer un cálculo rápido y preciso del número de clases de las forma cuadráticas binarias reducidas. Aunque no será nuestro objeto de estudio, interesa poner en conocimiento del lector una de sus aplicaciones. Recordar que una forma cuadrática binaria es un polinomio $f(x,y) \in \mathbb{Z}[x,y]$ homogéneo y de grado 2. Su forma general es $f(x,y) = ax^2 + bxy + cy^2$ y su discriminante se define por $D = b^2 - 4ac$. Si nos preocupamos - como ya hizo Euler - de expresiones menos generales, como puede ser $x^2 + Dy^2$, podemos establecer condiciones que permitan determinar qué números primos p son exactamente de la forma mencionada. Para $D = 1$, tenemos el problema clásico analizado por Fermat y resuelto con éxito en este documento. El anillo $\mathbb{Z}[i]$ nos proporciona la suficiente información como para asegurarnos de que sólo los primos impares de la forma $4n+1$ pueden ponerse como $x^2 + y^2$. El primo par 2 que claramente puede, pues $2 = 1^2 + 1^2$ jugará un papel especial, ya que es suma de dos cuadrados idénticos. No es difícil imaginar el porqué de nuestra conformidad, completando cuadrados $ax^2 + bxy + cy^2$ puede escribirse como $ax^2 + Dy^2$ tras aplicar el cambio de variable preciso.

Resulta gratificante retrotraerse a la época en que Fermat y Euler trataban de razonar con estos problemas con un enunciado tan sencillo que está al alcance de todos. Uno puede armarse de valor y a puro de fuerza bruta encontrar enteros que satisfagan cierta ecuación diofántica. Desafortunadamente, las matemáticas no se construyen así. Si se quieren tener resultados se necesitará cierto grado de sofisticación en los métodos y al menos un algoritmo con un coste computacional que consideremos razonable. Para tristeza de algunos o consuelo de otros, el décimo problema del milenio que consistía en encontrar un algoritmo que determine si una ecuación diofántica polinómica con coeficientes enteros tiene solución entera ya fue resuelto. El teorema de Matiyasevich (1970) implica que no existe tal algoritmo. No obstante, el noveno problema de Hilbert que consiste en encontrar la ley más general posible del teorema de reciprocidad en cualquier cuerpo numérico algebraico se encuentra parcialmente resuelto por Artin para las extensiones abelianas de los números racionales. Esto significa que para el caso no abeliano permanece abierto y puede ser todavía objeto de quebraderos de cabeza para los matemáticos con un interés elevado en resolverlo.

Sirvan pues estos capítulos como un acercamiento a toda la magia que envuelve al teorema áureo de Gauss y siendo como son tan escuetos por la condición de Trabajo de Fin de Grado que se les confiere, al menos que sea un acercamiento liviano que satisfaga las curiosidades más inmediatas.

Abstract

In the present work we provide the reader an approach to the Quadratic Reciprocity Law (QRL). Gauss wrote that "mathematics is the queen of sciences and number theory is the queen of mathematics". Much of modern number theory goes around problems related to prime numbers. Indeed, the law of quadratic reciprocity is a theorem about modular arithmetic that gives conditions for the solvability of quadratic equations modulo prime numbers.

The *first part*, consisting of basic mathematics to handle QRL, is incredibly useful, and that is where the emphasis must be. It gives necessary tools to understand one of the most well-known proofs of the law of quadratic reciprocity stated in the ring of integers. We refer to Gauss' sixth proof based on Gauss sums. QRL is stated as presented by Legendre, so that we must first introduce a formula for whether a given integer a is a quadratic residue modulo a given prime number p.

Euler's Criterion. Let p be an odd prime and a a unit in $\mathbb{Z}_p$. Then a is a quadratic residue modulo p if and only if $a^{\frac{1}{2}(p-1)} \equiv 1 \pmod{p}$ and a quadratic non-residue if and only if $a^{\frac{1}{2}(p-1)} \equiv -1 \pmod{p}$.

This encourages the symbolism due to Legendre

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if there exists } x \in \mathbb{Z} \text{ such that } x^2 \equiv a \pmod{p} \\ -1 & \text{otherwise} \end{cases}$$

Once we define the Legendre symbol we are actually ready to formally state the QRL. But even before then, we can mention that given two odd primes p and q, QRL establishes an amazingly simple relationship between the Legendre symbol $\left(\frac{p}{q}\right)$ and its "reciprocal" $\left(\frac{q}{p}\right)$.

Quadratic Reciprocity Law. If p, q are two distinct odd prime numbers, then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{4}(p-1)(q-1)}$$

This is such a very compact formula that no one can deny its beauty. Nevertheless, it is usually stated in a meaningful way showing more precisely how the two Legendre symbols behave depending on whether each of them has the form $4n+1$ or $4n+3$.

$$\left(\frac{q}{p}\right) = \begin{cases} -\left(\frac{p}{q}\right) & \text{if } p \equiv 3 \text{ and } q \equiv 3 \pmod{4} \\ \left(\frac{p}{q}\right) & \text{if } p \equiv 1 \text{ or } q \equiv 1 \pmod{4} \end{cases}$$

In order to study other desirable scenarios in which QRL can be stated, we show an examination of this law depending on the ring of Gaussian integers which is a preliminary step to its general, i.e, the ring of quadratic integers. Through this investigation we aim to gain a better understanding of the applications of the law of quadratic reciprocity.

The *second part*, consisting of QRL applied to Gaussian integers, is amazingly connected with the one we write for $\mathbb{Z}$. Describing properly units and primes in $\mathbb{Z}[i]$, we turn out that $\mathbb{Z}[i]$ is in many ways analogous to $\mathbb{Z}$. For instance, Gaussian integers factor uniquely into primes elements.

Fermat claims about the quadratic form x^2+y^2 that odd primes of the form $4n+1$ are always of the form x^2+y^2, and that no number of the form $4n+3$ can ever be a divisor of a number of the form x^2+y^2. Rephrased in the language of quadratic residues, we say that -1 is a quadratic residue modulo primes of the form $4n+1$, and a quadratic non-residue modulo primes of the form $4n+3$. There is no apparent connection with primes in $\mathbb{Z}$ that can be represented as the sum of two squares and primes in $\mathbb{Z}[i]$. However, primes of the form $4n+3$ which cannot be of the form x^2+y^2 are Gaussian primes and primes of the form $4n+1$ are not. Our guess is that the factorization of an odd prime number p in the Gaussian integers is actually related to the quadratic form x^2+y^2.

- If $p \equiv 3 \pmod 4$, i.e, $p \neq x^2+y^2$, then it is a Gaussian prime.
- If $p \equiv 1 \pmod 4$, i.e, $p = x^2+y^2$, then it is the product of a Gaussian prime by its conjugate.

This equation x^2+y^2 is only a particular expression of a more general quadratic form x^2+Dy^2. Accordingly, one may state that, if primes dividing x^2+y^2 are the only having -1 as a quadratic residue modulo p, prime divisors p dividing x^2+Dy^2 are precisely the odd primes p for which $-D$ is a nonzero quadratic residue modulo p.

The *third part*, consisting of QRL applied to quadratic integers, is intimately tied up with reciprocity and congruences as it implies that the splitting behaviour of a prime p in a quadratic field depends only on p modulo D, where D is the field discriminant.

In algebraic number theory, a quadratic field is an algebraic number field K of degree two over $\mathbb{Q}$. Given a field K we define its ring of algebraic integers $\mathscr{O}_K$.

$$\mathscr{O}_K = \{ \ \alpha \in K \ \mid \ \exists \ 0 \neq f(x) \in \mathbb{Z}[X] \ \text{ such that } \ f(\alpha) = 0 \ \}$$

We aim to develop several basic properties of $\mathscr{O}_K$. In order to do so, we summarize different facts for quadratic field extensions. For instance, $\mathscr{O}_K$ preserves some properties of $\mathbb{Z}$, such as every non zero proper ideal admits unique factorization into a product of nonzero prime ideals. Nonetheless, $\mathscr{O}_K$ is not always a principal ideal domain, so may not admit unique factorization into a product of nonzero prime elements. In this regard, one of the fundamental ideas of algebraic number theory is to regain unique factorization in number fields by passing from elements to ideals. One might also think about quadratic congruences $x^2+bx+c \pmod p$ or, rearranging, $(x+\frac{b}{2})^2 \equiv \frac{b^2-4c}{4} \pmod p$. The original quadratic congruence is solvable if and only if its discriminant $D=b^2-4c$ is a square modulo p, so that $\left(\frac{D}{p}\right)=1$.

In this perspective, the ring of quadratic integers modulo a prime ideal is $\mathscr{O}_K/p\mathscr{O}_K \cong \mathbb{Z}_p[X]/(f(X))$ where $f(x)=X^2-X+\frac{1-D}{4}$ if $D \equiv 1 \pmod 4$. Therefore, p is prime in $\mathscr{O}_K$ if and only if $\mathbb{Z}_p[X]/(f(X))$ is a field (i.e., $f(X)$ is irreducible, $\left(\frac{D}{p}\right)=-1$). Given an odd prime p, it follows that:

- $p=\mathfrak{p}_1\mathfrak{p}_2$ is totally split in $\mathbb{Q}(\sqrt{D})$ if and only if $\left(\frac{D}{p}\right)=1$.
- p is inert in $\mathbb{Q}(\sqrt{D})$ if and only if $\left(\frac{D}{p}\right)=-1$.

There is also a third case concerning the splitting behaviour of a prime p in a quadratic field. We say that $p=\mathfrak{p}^2$ is ramified in $\mathbb{Q}(\sqrt{D})$ if and only if $D \mid p$. Naturally, we can also consider the case when $D \not\equiv 1 \pmod 4$ or even prime $p=2$ and a comprehensive analysis will be done throughout this work.

Índice general

Capítulo 1

La ley de reciprocidad cuadrática en $\mathbb{Z}$

El objetivo fundamental de este capítulo es introducir los elementos necesarios que permiten demostrar el notable resultado de Gauss, llamado Ley de Reciprocidad Cuadrática o Teorema Aúreo. Esta ley afirma que si p y q son primos, ninguno de ellos $\equiv 1 \pmod 4$, entonces p es un resto o no-resto cuadrático de q, según q sea un no-resto o resto cuadrático de p (en ese orden) mientras que si alguno de los primos $\equiv 1 \pmod 4$, o bien ambos son restos cuadráticos o bien ninguno de los dos lo es. Detallaremos a continuación a qué nos referimos con resto y no-resto y terminaremos el capítulo dando una elegante demostración de dicha ley basada en las sumas de raíces primitivas de la unidad.

1.1. Restos cuadráticos

Dado $n \in \mathbb{Z}$ un entero positivo, consideraremos el anillo $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$. Así, para cada $a \in \mathbb{Z}$ denotaremos $\bar{a} = a + n\mathbb{Z}$, con lo que $a \equiv b \pmod n$ si y sólo si $\bar{a} = \bar{b}$. Si no hay lugar a error llamaremos también a al elemento $\bar{a} \in \mathbb{Z}_n$. Asimismo, emplearemos (a,n) para refirnos al máximo común divisor entre a y n. Si p es un primo, $\mathbb{Z}_p$ es cuerpo y sus unidades forman un grupo de orden $p-1$.

En un cuerpo K, una raíz primitiva n-ésima de la unidad es un elemento ζ tal que es raíz n-ésima, es decir, $\zeta^n = 1$, y no es k-raíz de la unidad para ningún $k < n$. Como un polinomio de grado n tiene a lo más n raíces en K, si ζ es raíz primitiva n-ésima de la unidad, se tiene que las raíces de $X^n - 1$ son el subgrupo multiplicativo generado por ζ, es decir, $< \zeta >$. Supongamos ahora que $X^n - 1$ se escinde en K. Si la característica no divide a n, las raíces son distintas y forman un grupo multiplicativo. Si d divide a n, los elementos del grupo de orden divisor de d son las raíces de $X^d - 1$, que son d a lo sumo. Así, el grupo de las raíces sólo puede tener un subgrupo de orden d para cada divisor del orden del grupo y por tanto es cíclico y existen raíces n-ésimas primitivas de la unidad. En el caso del cuerpo Z_p, las unidades forman un grupo multiplicativo de orden $p-1$, luego, tienen orden divisor de $p-1$ y son exactamente las raíces de $X^{p-1} - 1$. Así, forman un grupo cíclico que denotaremos C_{p-1} y a los generadores, que son las $p-1$ raíces primitivas de la unidad en el cuerpo Z_p, los llamaremos raíces primitivas módulo p.

Notación 1.1.1 (Símbolo de Legendre)**.** Sea $p \in \mathbb{Z}$ un primo impar y a una unidad de $\mathbb{Z}_p$. Se define el símbolo de Legendre $\left(\frac{a}{p}\right)$ correspondiente al par (a,p) como sigue:

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{si existe } x \in \mathbb{Z} \text{ tal que } x^2 \equiv a \pmod p \\ -1 & \text{en otro caso} \end{cases}$$

En las condiciones anteriores, a se dirá *resto cuadrático* $\pmod p$ si $\left(\frac{a}{p}\right) = 1$. En caso contrario, a se dirá *no-resto cuadrático* $\pmod p$. Esta definición podría extenderse al conjunto de los números naturales tomando $n \in \mathbb{N}$ en lugar de $p \in \mathbb{Z}$ primo impar. Sin embargo, nuestro interés reside exclusivamente en los números primos, por lo que no consideraremos este caso. En particular, decir que existe $x \in Z$ tal que $x^2 \equiv a \pmod p$ equivale a decir que a tiene una raíz cuadrada en $\mathbb{Z}_p$.

Notar que ser un resto cuadrático o un no-resto cuadrático es en realidad una propiedad de la clase $a \in \mathbb{Z}_p$, de modo que:

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \quad \text{si} \quad a \equiv b \pmod{p}$$

Observación 1.1.2. Si p divide a a, $a \equiv 0 \pmod{p}$ y se toma por convenio $\left(\frac{a}{p}\right) = 0$.

1.2. Raíces primitivas módulo p

Al ser C_{p-1} un grupo cíclico de orden $p-1$, $C_{p-1} = \{1, g, g^2, , \ldots , g^{\frac{p-1}{2}}, g^{\frac{p+1}{2}}, \ldots, g^{p-3}, g^{p-2}\}$ y decir que g es una raíz primitiva $\pmod{p}$ equivale a decir que su orden es $p-1$ en C_{p-1}. En general, dado que cada elemento distinto de cero de $\mathbb{Z}_p$ puede escribirse como $g^a \pmod{p}$ para algún entero a, también la ecuación $x^k \equiv y \pmod{p}$ puede escribirse como $(g^a)^k \equiv g^b \pmod{p}$ o $g^{ak-b} \equiv 1 \pmod{p}$. Como g es una raíz primitiva, y esto sucede si y solo si $(p-1) \mid (ak-b)$, entonces $ak \equiv b \pmod{(p-1)}$. Notar que y es potencia k-ésima si y sólo si $y \in < g^k >$ y este subgrupo tiene tantos divisores como el orden de g^k que es exactamente $\dfrac{p-1}{(k, p-1)}$. En particular, si $k = p-1$, se tiene el pequeño teorema de Fermat ($a^{(p-1)} \equiv 1 \pmod{p}$). Por otro lado, si $k = 2$, se tiene el número de restos cuadráticos $\pmod{p}$.

Proposición 1.2.1. *Sea p un primo impar. Si g es una raíz primitiva módulo p, entonces g^k es un resto cuadrático módulo p si k es par, y un no-resto cuadrático módulo p si k es impar, de modo que:*

$$\left(\frac{g^k}{p}\right) = (-1)^k$$

Demostración. Concretaremos lo ya mencionado para el caso $k = 2$. En primer lugar, fijaremos $k \in \mathbb{Z}$ para poder tomar $a = g^k$ en $\mathbb{Z}_p$, con $g \in \mathbb{Z}$ raíz primitiva módulo p. Supongamos ahora que g^k es un resto cuadrático módulo p, en tal caso existirá $x \in \mathbb{Z}$ tal que $x^2 \equiv g^k$ módulo p. Podemos asumir sin pérdida de generalidad que $x = g^l$ en $\mathbb{Z}_p$ para cierta $l \in \mathbb{Z}$, y así, $g^k = g^{2l}$ en $\mathbb{Z}_p$, es decir, $2l$ es congruente con k módulo $p-1$ y por ser $p-1$ par, k es par. Es evidente que en el caso en que a fuese no-resto cuadrático módulo p, $2 \nmid k$, y entonces k impar.

□

Corolario 1.2.2. *En C_{p-1}, hay $\frac{1}{2}(p-1)$ restos cuadráticos y otros tantos no-restos cuadráticos.*

Demostración. Por la proposición anterior, las clases correspondientes a las potencias pares de g son restos cuadráticos módulo p, y las que corresponden a las impares no-restos cuadráticos módulo p. □

Corolario 1.2.3. *El símbolo de Legendre tiene función multiplicativa. Dados $a, b \in \mathbb{Z}$ se sigue que:*

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$$

Demostración. Si g es una raíz primitiva módulo p, existen k, $l \in \mathbb{Z}$ tales que $a = g^k$ y $b = g^l$ en $\mathbb{Z}_p$.

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{g^k}{p}\right)\left(\frac{g^l}{p}\right) = (-1)^k(-1)^l = (-1)^{k+l} = \left(\frac{ab}{p}\right)$$

□

1.3. Criterio de Euler

Enunciaremos ahora un primer criterio que proporciona una condición necesaria y suficiente para ver si un entero $a \neq 0 \pmod{p}$ es un resto cuadrático o un no-resto cuadrático módulo p. Por su conveniencia, daremos dos demostraciones equivalentes, una empleando raíces primitivas módulo p y otra apoyándonos en resultados de la teoría de grupos.

Lema 1.3.1 (Criterio de Euler)**.** *Sea p un primo impar, entonces:*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{1}{2}(p-1)} \pmod{p}$$

Demostración. I. Supongamos primero que p no divide a a, fijaremos $k \in \mathbb{Z}$ para poder tomar $a = g^k$ en $\mathbb{Z}_p$ con g raíz primitiva módulo p.

$$a^{\frac{1}{2}(p-1)} \equiv g^{k\frac{1}{2}(p-1)} \pmod{p}$$

Tomando $b = g^{\frac{1}{2}(p-1)}$, notamos que $b^2 = g^{p-1} = 1$ en $\mathbb{Z}_p$ y así $b = \pm 1$. Pero como g es una raíz primitiva, $b \neq 1$ (si fuese $b = 1$, entonces el orden de g sería menor o igual que $\frac{1}{2}(p-1)$ y esto no es posible). Luego $b = -1$ y por la Proposición 1.2.1:

$$a^{\frac{1}{2}(p-1)} \equiv (-1)^k \equiv \left(\frac{g^k}{p}\right) = \left(\frac{a}{p}\right) \pmod{p}$$

Finalmente, si p divide a a, el teorema se verifica trivialmente pues p divide a $a^{\frac{1}{2}(p-1)}$.

□

Demostración. II. Considérese el grupo cíclico C_{p-1}. Notar que el orden de cada elemento a es un divisor del orden del grupo $p-1$ y así, $a^{(p-1)} = 1$ en $\mathbb{Z}_p$. Señalado esto, $(a^{\frac{1}{2}(p-1)})^2 = a^{(p-1)} = 1$ en $\mathbb{Z}_p$, luego, o bien, $a^{\frac{1}{2}(p-1)} = 1$ o bien, es un elemento de orden 2. No obstante, en un grupo cíclico de orden $p-1$ solo existe un elemento de orden 2 que en nuestro caso particular es $p-1 = -1$. Sea g un generador de C_{p-1} ($|< g >| = p-1$), el único subgrupo de orden $\frac{1}{2}(p-1)$ es $< g^2 >$. Sea ahora d el orden de a en C_{p-1}, notar que $a^{\frac{1}{2}(p-1)} = 1$ si y sólo si el orden d es un divisor de $\frac{1}{2}(p-1)$. Esto se tiene si y sólo si $< g^2 >$ tiene un subgrupo de orden d, y por ser único el subgrupo de orden d en C_{p-1}, $< a > \leq < g^2 >$. Esto ocurre si y sólo si existe k tal que $a = (g^2)^k$ si y sólo si para algún k, $a = (g^k)^2$ si y solo si existe $g = g^k \in C_{p-1}$ tal que $a = g^2$. □

La aplicación $\left(\frac{\cdot}{p}\right) : C_{p-1} \to \{\pm 1\}$, $a \mapsto a^{\frac{1}{2}(p-1)}$ es homomorfismo de grupos y por tanto tiene función multiplicativa. Sean ahora $a, b \in \mathbb{C}_{p-1}$, se sigue:

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = a^{\frac{1}{2}(p-1)} b^{\frac{1}{2}(p-1)} = ab^{\frac{1}{2}(p-1)} = \left(\frac{ab}{p}\right) \pmod{p}$$

Además, este homomorfismo tiene por núcleo el único subgrupo de orden 2, $Ker\left(\frac{\cdot}{p}\right) = < g^2 >$ y su imagen es un grupo cíclico de orden 2, es decir, $Im\left(\frac{\cdot}{p}\right) = \{-1, 1\}$. En particular, la aplicación es suprayectiva pues exactamente la mitad de los elementos de C_{p-1} (los que provienen de $< g^2 >$) son restos cuadráticos y la otra mitad no.

Observación 1.3.2. Usando el Criterio de Euler, puede deducirse que una raíz primitiva módulo p es un no-resto cuadrático módulo p (notar que el orden de un resto cuadrático módulo p divide a $\frac{p-1}{2}$ pero una raíz primitiva tiene orden $p-1 \not\leq \frac{p-1}{2}$, luego necesariamente es un no-resto cuadrático).

Ejemplo 1.3.3. Por el Lema 1.3.1, para obtener el símbolo de Legendre de una unidad a de $\mathbb{Z}_p$ basta ver con qué elemento es congruente $a^{\frac{1}{2}(p-1)}$ en $\mathbb{Z}_p$. En particular, en $\mathbb{Z}_{13}$,

$$\left(\frac{8}{13}\right) = 8^6 = (-5)^6 = (5^2) = (-1)^3 = -1$$

El Criterio de Euler nos dice que para determinar si -1 es un resto cuadrático o un no-resto cuadrático módulo p sólo es necesario considerar primos $(\text{mód } 4)$. Daremos dos demostraciones de este hecho, una cuasi-inmediata y otra apoyándonos en raíces primitivas de la unidad. Por cuasi-inmediata entendemos aquella que es meramente combinatoria y no precisa métodos más sofisticados, en contraposición a otras que involucran herramientas que precisan un grado de abstracción mayor.

Corolario 1.3.4 (Primera ley suplementaria)**.** *Sea p un primo impar, entonces -1 es resto cuadrático módulo p si y sólo si $p \equiv 1 \pmod 4$ y no-resto cuadrático módulo p si y sólo si $p \equiv 3 \pmod 4$.*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & si \quad p \equiv 1 \pmod 4 \\ -1 & si \quad p \equiv 3 \pmod 4 \end{cases}$$

Demostración. I. Por el Lema 1.3.1, basta analizar la paridad del exponente $\frac{1}{2}(p-1)$. Consideremos las únicas 2 posibilidades de un primo impar $p \pmod 4$.

- $\mathbf{p = 4k+1}$. $\quad \frac{1}{2}(p-1) = 2k, \quad \left(\frac{-1}{p}\right) = (-1)^{2k} = 1.$
- $\mathbf{p = 4k+3}$. $\quad \frac{1}{2}(p-1) = 2k+1, \quad \left(\frac{-1}{p}\right) = (-1)^{2k+1} = -1.$

□

Demostración. II. Sea ζ una raíz primitiva cuarta de la unidad en una extensión de cuerpos de $\mathbb{Z}_p$ de característica p. Notar que $\zeta^4 - 1 = (\zeta^2+1)(\zeta^2-1) = 0$. Por ser ζ raíz primitiva cuarta, $\zeta^2 - 1 \neq 0$ pues $\zeta^2 \neq 1$ y necesariamente $\zeta^2 = -1$. Sea $x = \zeta$ el elemento que verifica $x^2 = -1$

$$x^{p-1} = (x^2)^{\frac{1}{2}(p-1)} = (-1)^{\frac{1}{2}(p-1)} \equiv \left(\frac{-1}{p}\right) \pmod p$$

- Si $p = 1 \pmod 4$, entonces $x^p = \zeta^p = \zeta^{4k+1} = \zeta = x, \quad \left(\frac{-1}{p}\right) = x^{p-1} = 1.$
- Si $p = 3 \pmod 4$, entonces $x^p = \zeta^p = \zeta^{4k+3} = \zeta^3 = -\zeta = -x, \quad \left(\frac{-1}{p}\right) = x^{p-1} = -1.$

□

El nombre de primera ley suplementaria (respecto a la ley de reciprocidad cuadrática) no es casual. Una pregunta frecuente que surge en la teoría de números es cómo evaluar cierto símbolo de Legendre $\left(\frac{a}{p}\right)$ para un cierto $a \in \mathbb{Z}$. La ley de reciprocidad cuadrática nos dice cómo hacerlo si a es impar y positivo pero queda pendiente saber cómo actuar frenta a $a < 0$. Ahí, es donde cobra importancia $\left(\frac{-1}{p}\right)$. Por otro lado, para a par, necesitaremos otra ley suplementaria adicional, es decir, $\left(\frac{2}{p}\right)$. Cuando enunciemos el lema de Gauss, esta segunda ley aparecerá como corolario y al final del capítulo mostraremos cómo unir todo para calcular cualquier símbolo de Legendre.

1.4. Sumas de Gauss

En esta subsección se presentan una serie de identidades algebraicas asociadas a sumas de raíces de la unidad. Ya adelantábamos al inicio del capítulo la importancia que tendrían estas raíces pues proporcionan una herramienta poderosa para probar tanto la ley de reciprocidad cuadrática como otras de grados superiores. Sin embargo, los objetos que presentaremos a continuación suscitan interés por sí mismos.

Definición 1.4.1. Sea $p \in \mathbb{Z}$ un primo impar , la suma de Gauss asociada a un elemento $a \neq 0 \in \mathbb{Z}$ es:

$$g_a = \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \zeta_p^{an} = \left(\frac{0}{p}\right) + \left(\frac{1}{p}\right)\zeta_p^a + \ldots + \left(\frac{p-2}{p}\right)\zeta_p^{a(p-2)} + \left(\frac{p-1}{p}\right)\zeta_p^{a(p-1)}$$

donde ζ_p es una raíz p-primitiva de la unidad en el cuerpo $\mathbb{C}$, i.e., $\zeta_p = e^{\frac{2\pi i}{p}} = \cos\frac{2\pi}{p} + i\,\mathrm{sen}\,\frac{2\pi}{p}$.

Téngase en cuenta que p está implícito en la definición de g_a. Si cambiáramos p, entonces la suma de Gauss g_a asociada a a sería diferente. La definición de g_a también depende de nuestra elección de ζ. Por comodidad, fijaremos p y denotaremos $\zeta_p = \zeta$ en lo sucesivo.

Observación 1.4.2. En particular, se toma por convenio $g_0 = 0$ y así $g_1 = \left(\frac{a}{p}\right) g_a$.

Es claro que $g_0 = \sum_{n=0}^{p-1} \left(\frac{n}{p}\right)$, con lo cual, sabiendo que $\left(\frac{0}{p}\right) = 0$ y $\left(\frac{\cdot}{p}\right) : C_{p-1} \to \{\pm 1\}$, de modo que $a \mapsto a^{\frac{1}{2}(p-1)}$ es epimorfismo, se sigue $g_0 = 0$. Por otro lado, $g_1 = \sum_{n=0}^{p-1} \left(\frac{n}{p}\right)\zeta^n$ y supongamos que $a \neq 0$ en $\mathbb{Z}_p$ (si fuese $a = 0$, $g_1 = 0$), entonces $\left(\frac{a}{p}\right) g_a = \left(\frac{a}{p}\right)\sum_{n=0}^{p-1}\left(\frac{n}{p}\right)\zeta^{an} = \sum_{n=0}^{p-1}\left(\frac{an}{p}\right)\zeta^{an} = \sum_{k=0}^{p-1}\left(\frac{k}{p}\right)\zeta^k = g_1$.

Notar además que si $g_1 = \left(\frac{a}{p}\right) g_a$, se sigue que $\left(\frac{a}{p}\right) g_1 = \left(\frac{a}{p}\right)^2 g_a = g_a$ y tenemos una expresión para g_a en función de g_1. Nos centraremos ahora en encontrar una expresión adecuada y manejable para el cuadrado de una suma de Gauss, es decir, buscamos expresar $g_a^2 = g_1^2$ convenientemente.

Lema 1.4.3.

$$\sum_{n=0}^{p-1} \zeta^{an} = \begin{cases} p & \text{si } a \equiv 0 \pmod{p} \\ 0 & \text{en otro caso} \end{cases}$$

Demostración.

- Si $a \equiv 0 \pmod{p}$, $\sum_{n=0}^{p-1} \zeta^{an} = \sum_{n=0}^{p-1} 1 = (p-1) + 1 = p$.
- Si $a \not\equiv 0 \pmod{p}$, $\zeta^{ap} - 1 = (\zeta^a - 1)(\zeta^{a(p-1)} + \ldots + \zeta^a + 1) = (\zeta^a - 1)\sum_{n=0}^{p-1}\zeta^{an}$.
  Como $\zeta^a \neq 1$, $\zeta^a - 1 \neq 0$,
  $$\sum_{n=0}^{p-1} \zeta^{an} = \frac{\zeta^{ap} - 1}{\zeta^a - 1} = \frac{1-1}{\zeta^a - 1} = 0$$

□

Es importante señalar que $a \in \mathbb{Z}$ puede reescribirse en términos de otros dos enteros $x, y \in \mathbb{Z}$, que en caso de satisfacer $x = y$ en $\mathbb{Z}_p$, proporcionan $\sum_{n=0}^{p-1} \zeta^{(x-y)n} = p$ y en caso contrario, $\sum_{n=0}^{p-1} \zeta^{(x-y)n} = 0$.

Proposición 1.4.4. *Sea $a \not\equiv 0 \pmod{p}$,*

$$g_a^2 = (-1)^{\frac{p-1}{2}} p = \left(\frac{-1}{p}\right) p$$

Demostración. Por un lado, a partir de la expresión para g_a siguiendo la Observación 1.4.2 se tiene

$$\sum_{a=0}^{p-1} g_a g_{-a} = \sum_{a=0}^{p-1} \left(\frac{a}{p}\right) g_1 \left(\frac{-a}{p}\right) g_1 = \sum_{a=0}^{p-1} \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right)^2 g_1^2 = \sum_{a=0}^{p-1} (-1)^{\frac{p-1}{2}} g_1^2 = (p-1)(-1)^{\frac{p-1}{2}} g_1^2$$

Por otro lado, aplicando directamente la Definición 1.4.1

$$\sum_{a=0}^{p-1} g_a g_{-a} = \sum_{a=0}^{p-1} \left(\sum_{n=0}^{p-1} \left(\frac{n}{p}\right)\zeta^{an} \sum_{k=0}^{p-1} \left(\frac{k}{p}\right)\zeta^{ak} \right) = \sum_{n=0}^{p-1}\sum_{k=0}^{p-1} \left(\frac{n}{p}\right)\left(\frac{k}{p}\right) \sum_{a=0}^{p-1} \zeta^{a(n-k)}$$

Ahora bien, por el Lema 1.4.3, $\sum_{a=0}^{p-1} \zeta^{a(n-k)} = p$ si $n = k$ en $\mathbb{Z}_p$ y 0 en caso contrario.

Recapitulando,

$$\sum_{a=0}^{p-1} g_a g_{-a} = \sum_{n=0}^{p-1}\sum_{k=0}^{p-1}\left(\frac{n}{p}\right)\left(\frac{k}{p}\right)p = \sum_{n=0}^{p-1}\left(\frac{n}{p}\right)^2 p = \sum_{n=0}^{p-1} p = (p-1)p = (p-1)(-1)^{\frac{1}{2}(p-1)}g_1^2$$

Cancelando $p-1$ y multiplicando por $(-1)^{\frac{p-1}{2}}$ en ambos miembros, se tiene la expresión buscada

$$g_a^2 = g_1^2 = (-1)^{\frac{1}{2}(p-1)}p$$

□

Corolario 1.4.5.

$$g_a = \begin{cases} \pm\sqrt{p} & si\ p \equiv 1 \pmod 4 \\ \pm i\sqrt{p} & si\ p \equiv 3 \pmod 4 \end{cases}$$

Demostración. Notar que $g_a^2 = \left(\frac{-1}{p}\right)p = p$ si $p \equiv 1 \pmod 4$ y $g_a^2 = \left(\frac{-1}{p}\right)p = -p$ si $p \equiv 3 \pmod 4$. Por la primera ley suplementaria 1.3.4, existe $x \in Z$ tal que $x^2 \equiv -1 \pmod p$ si $p \equiv 1 \pmod 4$ y no existe tal $x \in Z$ si $p \equiv 1 \pmod 3$. Así, $g_a = \pm\sqrt{p}$ si existe y $g_a = \pm i\sqrt{p}$ en caso contrario.

Ejemplo 1.4.6. (Cálculo la suma de Gauss para $p = 7$)

$$g_1 = \left(\frac{0}{7}\right) + \left(\frac{1}{7}\right)\zeta + \left(\frac{2}{7}\right)\zeta^2 + \left(\frac{3}{7}\right)\zeta^3 + \left(\frac{4}{7}\right)\zeta^4 + \left(\frac{5}{7}\right)\zeta^5 + \left(\frac{6}{7}\right)\zeta^6$$

Por definición, $\left(\frac{0}{7}\right) = 0$. Además, $\left(\frac{1}{7}\right) = 1$ pues $1^2 \equiv 1 \pmod p\ \forall\ p$. También $\left(\frac{2}{7}\right) = 1$ ya que $3^2 \equiv 2 \pmod 7$ y $\left(\frac{4}{7}\right) = 1$, pues $5^2 \equiv 4 \pmod 7$. Como ya hemos determinado los 3 restos cuadráticos módulo 7 (y no hay más, pues son exactamente la mitad de ellos), directamente se tiene $\left(\frac{3}{7}\right) = \left(\frac{4}{7}\right) = \left(\frac{6}{7}\right) = -1$.

$$g_1 = \zeta + \zeta^2 - \zeta^3 + \zeta^4 - \zeta^5 - \zeta^6 = \pm i\sqrt{7}$$

Calcularemos ahora la suma de Gauss al cuadrado para ver que efectivamente $g_1^2 = -7$.

$$\begin{aligned} g_1^2 &= \zeta^6 + \zeta^{-6} - 2\zeta^5 - 2\zeta^{-5} - \zeta^4 - \zeta^{-4} + 2\zeta^3 + 2\zeta^{-3} + 3\zeta^2 + 3\zeta^{-2} - 6 = \\ &= (1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6 - 1) - 6 = -1 - 6 = -7 \end{aligned}$$

Notar $\zeta^7 - 1 = (\zeta - 1)(1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6) = 0$ y $\zeta - 1 \neq 0$.

□

1.5. Lema de Gauss

El lema de Gauss - al igual que ocurría con el criterio de Euler - proporciona una condición necesaria y suficiente para ver si una unidad a de $\mathbb{Z}_p$ es o no un resto cuadrático módulo p. Este lema cobra cierto interés por estar involucrado en varias de las pruebas más conocidas de la ley de reciprocidad cuadrática. De hecho, hizo su primera aparición en la tercera prueba de Carl Friedrich Gauss (1808) y luego volvió a ser usado en la quinta prueba del mismo autor (1818).

Lema 1.5.1 (Lema de Gauss)**.** *Sea $p \in \mathbb{Z}$ un primo impar y a una unidad de $\mathbb{Z}_p$, si $I = \{1, \ldots, \frac{1}{2}(p-1)\}$, se tiene que $C_{p-1} = I \sqcup -I$ donde $-I = \{-i \mid i \in I\}$, y además:*

$$\left(\frac{a}{p}\right) = (-1)^n,\ \ n = \#\{j \in I \mid aj \in -I\}$$

Demostración. Notar que las unidades de $\mathbb{Z}_p = \{1,2,\ldots,p-1\}$ se dividen en dos subconjuntos disjuntos I y $-I$ siendo $I = \{1,2,\ldots,\frac{p-1}{2}\}$ y $-I$ el subconjunto de C_{p-1} formado por exactamente todas las unidades restantes, pues $-k = p-k$ en $\mathbb{Z}_p$. Por simplicidad, denotemos

$$J_- = \{j \in I \mid aj \in -I\}, \quad J_+ = \{j \in I \mid aj \in I\}$$

Afirmamos que J_- y J_+ son disjuntos y su unión es I (ya que a es una unidad e I y $-I$ son disjuntos). Sean ahora $-aJ_-, aJ_+ \subset I$ donde

$$-aJ_- = \{-aj_- \mid j_- \in J_-\}, \quad aJ_+ = \{aj_+ \mid j_+ \in J_+\}$$

Afirmamos esta vez que $-aJ_-$ y aJ_+ son disjuntos y su unión es I (si fuese $-aj_- = aj_+$ en $\mathbb{Z}_p$, entonces $-j_- = j_+$ y esto no es posible ya que $-j_- \in -I$ y $j_+ \in I$). Calculemos la cardinalidad de estos conjuntos.

$$\#\left(-aJ_- \sqcup aJ_+\right) = \#\left(J_- \sqcup J_+\right) = \#J_- + \#J_+ = \#I = \frac{1}{2}(p-1)$$

Entonces, el producto de elementos de I módulo p es

$$\prod_{j\in I} j = \prod_{j\in J_-}(-aj_-)\prod_{j\in J_+}(aj_+) \equiv a^{\frac{1}{2}(p-1)}(-1)^{\#J_-}\prod_{j\in J_-\,\sqcup\, J_+} j$$

Como señalábamos anteriormente, $I = J_- \sqcup J_+$, por lo que $\prod_{j\in I} j = \prod_{j\in J_-\,\sqcup\, J_+} j$, y entonces,

$$a^{\frac{1}{2}(p-1)} \equiv (-1)^{\#J_-} \pmod{p}$$

El resultado se tiene aplicando del Lema 1.3.1 ya que identificamos $a^{\frac{1}{2}(p-1)}$ con $\left(\frac{a}{p}\right)$. □

Ejemplo 1.5.2. Por el Lema 1.5.1, para obtener el símbolo de Legendre de una unidad a de $\mathbb{Z}_p$ basta calcular cuántos elementos del conjunto $aI = \{ai \mid i \in I\}$ están en $-I$. En particular, en $\mathbb{Z}_{13}$,

$$I = \{1,2,3,4,5,6\}, \quad 8I = \{8,16,24,32,40,48\} = \{-5,3,-2,6,1,-4\}$$

$$J_+ = \{2,4,5\}, \quad J_- = \{1,3,6\}, \quad n = \#\{j \in I \mid 8j \in -I\} = \#J_- = 3$$

$$\left(\frac{8}{13}\right) = (-1)^n = -1, \text{ concluimos que 8 no es resto cuadrático módulo 13.}$$

El Lema de Gauss nos dice que para determinar si 2 es un resto cuadrático o un no-resto cuadrático módulo p sólo es necesario considerar primos (mód 8). Daremos dos demostraciones de este hecho, una siguiendo fundamentalmente las ideas de la demostración del Lema 1.5.1 y otra apoyándonos en raíces primitivas de la unidad.

Corolario 1.5.3 (Segunda ley suplementaria)**.** *Sea p un primo impar, entonces 2 es resto cuadrático módulo p si y sólo si $p \equiv \pm 1 \pmod 8$ y no-resto cuadrático módulo p si y sólo si $p \equiv \pm 3 \pmod 8$.*

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & si \quad p \equiv \pm 1 \pmod 8 \\ -1 & si \quad p \equiv \pm 3 \pmod 8 \end{cases}$$

Demostración. I. Consideremos las únicas 4 posibilidades de un primo impar p en $\mathbb{Z}_8$. Para ello, tomamos $p = 8k+2r+1$, $r \in \{0,1,2,3\}$, $I = \{1,2,\ldots,4k+r\}$ y $2I = \{2,4,\ldots,8k+2r\}$. Debemos identificar qué elementos $j \in I$ con $2j \in 2I$ pertenecen a I y cuáles a $-I$. Definimos J_+ y J_- como antes.

- Si r es par, J_+ y J_- tienen exactamente el mismo número de elementos.

$$J_+ = \{\ 1\ ,\ 2\ ,\ \ldots\ ,\ 2k+\frac{r}{2}\ \}, \quad J_- = \{\ 2k+\frac{r+2}{2}\ ,\ 2k+\frac{3r}{2}\ ,\ \ldots\ ,\ 4k+r\ \}$$

- Si r es impar, J_+ tiene exactamente un elemento menos que J_-.

$$J_+ = \{\ 1\ ,\ 2\ ,\ \dots\ ,\ 2k+\frac{r-1}{2}\ \},\quad J_- = \{\ 2k+\frac{r+1}{2}\ ,\ 2k+r\ ,\ \dots\ ,\ 4k+r\ \}$$

Recapitulando, el número de elementos de J_- según la paridad de r es:

$$n = \begin{cases} 2k+\dfrac{r}{2} \equiv \dfrac{r}{2} & (\text{mód } 2) \qquad \text{si r par} \\ 2k+\dfrac{r+1}{2} \equiv \dfrac{r+1}{2} & (\text{mód } 2) \qquad \text{si r impar} \end{cases}$$

Finalmente,

- $\mathbf{p = 8k+1}$. $\quad r=0,\quad \dfrac{r}{2}=0,\quad \left(\dfrac{2}{p}\right) = (-1)^0 = 1.$
- $\mathbf{p = 8k+3}$. $\quad r=1,\quad \dfrac{r+1}{2}=1,\quad \left(\dfrac{2}{p}\right) = (-1)^1 = -1.$
- $\mathbf{p = 8k+5}$. $\quad r=2,\quad \dfrac{r}{2}=1,\quad \left(\dfrac{2}{p}\right) = (-1)^1 = -1.$
- $\mathbf{p = 8k+7}$. $\quad r=3,\quad \dfrac{r+1}{2}=2,\quad \left(\dfrac{2}{p}\right) = (-1)^2 = 1.$

□

Demostración. II. Sea ζ una raíz primitiva octava de la unidad en una extensión de cuerpos de $\mathbb{Z}_p$ de característica p (i.e, $x^p = \zeta^p + \zeta^{-p}$). Notar que $\zeta^8 - 1 = (\zeta^4+1)(\zeta^4-1) = 0$. Por ser ζ raíz primitiva octava, $\zeta^4 - 1 \neq 0$ pues $\zeta^4 \neq 1$ y necesariamente $\zeta^4 + 1 = 0$. Multiplicando por ζ^{-2}, $\zeta^2 + \zeta^{-2} = 0$ y $(\zeta^1 + \zeta^{-1})^2 = \zeta^2 + \zeta^{-2} + 2 = 2$. Sea $x = \zeta + \zeta^{-1}$ el elemento que verifica $x^2 = 2$, entonces

$$x^{p-1} = (x^2)^{\frac{1}{2}(p-1)} = 2^{\frac{1}{2}(p-1)} \equiv \left(\frac{2}{p}\right) \quad (\text{mód } p)$$

.

- Si $p = \pm 1 \pmod 8$, entonces $x^p = \zeta + \zeta^{-1} = x$, $\quad \left(\dfrac{2}{p}\right) = x^{p-1} = 1.$
- Si $p = \pm 5 \pmod 8$, entonces $x^p = \zeta^5 + \zeta^{-5} = -(\zeta + \zeta^{-1}) = -x$, $\quad \left(\dfrac{2}{p}\right) = x^{p-1} = -1.$

□

1.6. La ley de reciprocidad cuadrática

Como bien señalábamos al inicio del Capítulo 1, la ley de reciprocidad cuadrática (Euler, 1783), afirma que si p y q son primos, ninguno de ellos $\equiv 1 \pmod 4$, entonces p es un resto o no-resto cuadrático de q, según q sea un no-resto o resto cuadrático de p (en ese orden) mientras que si alguno de los primos $\equiv 1 \pmod 4$, o bien ambos son restos cuadráticos o bien ninguno de los dos lo es. Este teorema se formuló de varias maneras: Euler y Legendre no tenían la notación de congruencia de Gauss, ni Gauss tenía el símbolo de Legendre. En esta sección emplearemos la formulación moderna que incorpora símbolos de Legendre y daremos una de las demostraciones basada en sumas de Gauss, más concretamente, la que se inspira en su sexta prueba. Para una visión conjuntista que se sustenta en argumentos puramente combinatorios y tiene por base al lema de Gauss, véase el Anexo I.

Teorema 1.6.1. *Sean p y q primos impares y distintos, entonces se verifica*

$$\left(\frac{q}{p}\right) = (-1)^{\frac{1}{4}(p-1)(q-1)} \left(\frac{p}{q}\right)$$

Demostración. Sea q un primo impar con $q \neq p$ y denotemos $p^* = (-1)^{\frac{1}{2}(p-1)} p = g_1^2 = \left(\sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \zeta^n\right)^2$. En particular, aplicando el Criterio de Euler 1.3.1,

$$(p^*)^{\frac{1}{2}(q-1)} \equiv \left(\frac{p^*}{q}\right) \pmod{q}, \text{ o equivalentemente, } g_1^{q-1} \equiv \left(\frac{p^*}{q}\right) \pmod{q}$$

Nos centraremos en la congruencia que resulta de multiplicar ambos miembros por g_1,

$$g_1^q \equiv \left(\frac{p^*}{q}\right) g_1 \pmod{q}$$

La cuestión ahora radica en interpretar adecuadamente dicha congruencia puesto que $g_1^q \notin \mathbb{Z}$. Así, decir que $g_1^q \equiv g_1 \left(\frac{p^*}{q}\right) \pmod{q}$ equivale a decir que la diferencia $g_1^q - g\left(\frac{p^*}{q}\right) \in (q)$ siendo (q) un ideal del anillo $\mathbb{Z}[\zeta]$ de todos los polinomios en ζ con coeficientes en $\mathbb{Z}$. El anillo cociente $\mathbb{Z}[\zeta]/(q)$ tiene característica q, luego si $x, y \in \mathbb{Z}[\zeta]$, entonces $(x+y)^q \equiv x^q + y^q \pmod{q}$. Aplicando esto, vemos que

$$\begin{aligned} g_1^q &= \left(\sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \zeta^n\right)^q \equiv \sum_{n=0}^{p-1} \left(\frac{n}{p}\right)^q \zeta^{nq} \pmod{q} \equiv \sum_{n=0}^{p-1} \left(\frac{n}{p}\right) \zeta^{nq} \pmod{q} \\ &\equiv g_q \pmod{q} \equiv \left(\frac{q}{p}\right) g_1 \pmod{q} \equiv \left(\frac{p^*}{q}\right) g_1 \pmod{q} \end{aligned}$$

Como $g^2 = p^*$ y $p \neq q$, podemos cancelar g_1 en ambos miembros y así $\left(\frac{q}{p}\right) \equiv \left(\frac{p^*}{q}\right) \pmod{q}$. Dado que ambos son símbolos de Legendre y q es impar, se deduce que $\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right)$.

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right) = \left(\frac{(-1)^{\frac{1}{2}(p-1)} p}{q}\right) = \left(\frac{-1}{q}\right)^{\frac{1}{2}(p-1)} \left(\frac{p}{q}\right) = (-1)^{\frac{1}{2}(q-1)\frac{1}{2}(p-1)} \left(\frac{p}{q}\right)$$

□

Esta demostración se puede adaptar con cierta facilidad para determinadas leyes que generalizan la ley de reciprocidad cuadrática, esto es, aquellas relativas a residuos cúbicos y residuos bicuadráticos, pero no trataremos esa cuestión. En lo que a nosotros respecta, se espera una expresión más manejable de la L.R.C. tal como dicta el corolario que enunciaremos a continuación.

Corolario 1.6.2. *Sean p y q primos impares y distintos, entonces p es un resto o no-resto cuadrático de q según q sea un no-resto o resto cuadrático de p (en ese orden) si y sólo si $p \equiv 3$ y $q \equiv 3 \pmod{4}$. En otro caso, p es un resto o no-resto cuadrático de q según q sea un resto o no-resto cuadrático de p.*

$$\left(\frac{q}{p}\right) = \begin{cases} -\left(\frac{p}{q}\right) & \text{si } p \equiv 3 \text{ y } q \equiv 3 \pmod{4} \\ \left(\frac{p}{q}\right) & \text{si } p \equiv 1 \text{ o } q \equiv 1 \pmod{4} \end{cases}$$

Demostración. Aplicaremos el Criterio de Euler 1.3.1 teniendo presente que las únicas dos posibilidades de un primo impar p en $\mathbb{Z}_4$ son $p = 4k+1$ y $p = 4k+3$.

- $\mathbf{p = 4k+1}$

$$\left(\frac{-1}{q}\right)^{\frac{1}{2}(p-1)} = \left(\frac{-1}{q}\right)^{2k} = 1 \quad \text{si} \quad q = 4k+1 \text{ ó } q = 4k+3$$

- $\mathbf{p = 4k+3}$

$$\left(\frac{-1}{q}\right)^{\frac{1}{2}(p-1)} = \left(\frac{-1}{q}\right)^{2k+1} = (-1)^{\frac{1}{2}(q-1)} = \begin{cases} 1 & \text{si } \ q = 4k+1 \\ -1 & \text{si } \ q = 4k+3 \end{cases}$$

□

Ejemplo 1.6.3. La ley de reciprocidad cuadrática es útil en el cálculo de los símbolos de Legendre. Sean $p = 7$, $q = 71$ dos números primos impares distintos, notar que $p \equiv 3$ y $q \equiv 3 \pmod 4$.

$$\left(\frac{7}{71}\right) = -\left(\frac{71}{7}\right) = -\left(\frac{1}{7}\right) = -1$$

Así, 7 no es un resto cuadrático módulo 71 y sin embargo, 71 es un resto cuadrático módulo 7. No obstante, no conocemos a priori $x \in \mathbb{Z}$ tal que $x^2 \equiv 71 \pmod 7$, sólo podemos asegurar que existe.

A modo de síntesis, señalaremos las propiedades útiles (1.2.3, 1.3.4, 1.5.3, 1.6.2) para el cálculo efectivo de los símbolos de Legendre. Es claro que basta factorizar $a = k\, 2^{k_0} q_1^{k_1} \dots q_s^{k_s}$, $\quad k = \pm 1$.

$$\left(\frac{a}{p}\right) = \left(\frac{k}{p}\right) \left(\frac{2}{p}\right)^{k_0} \left(\frac{q_1}{p}\right)^{k_1} \dots \left(\frac{q_s}{p}\right)^{k_s}$$

Ejemplo 1.6.4. La ley de reciprocidad cuadrática proporciona criterios útiles para ver si ciertas ecuaciones son resolubles. Si tomamos p y q dos primos impares distintos, y observamos la ecuación $p = x^2 + qy^2$, en particular, podemos reducir módulo p y obtener una condición necesaria para que dicha ecuación sea resoluble, es decir, $\left(\frac{-q}{p}\right) = 1$. De hecho, las leyes suplementarias vienen a complementar estas interacciones, pues aplicando el Corolario 1.3.4, se deduce que $p = x^2 + y^2$ si y sólo si $p \equiv 1 \pmod 4$, es decir, $\left(\frac{-1}{p}\right) = 1$ y aplicando el Corolario 1.5.3, $p = x^2 + 2y^2$ si y sólo si $p \equiv \pm 1 \pmod 8$, es decir, $\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = 1$. El análisis exhaustivo de tales cuestiones lo veremos más adelante.

Capítulo 2

La ley de reciprocidad cuadrática en $\mathbf{Z[i]}$

En este capítulo analizaremos un anillo particularmente famoso, el de los enteros gaussianos. Concretamente, Gauss encontró que la ley de reciprocidad cuadrática puede plantearse utilizando dichos enteros y la enunció en el anillo $\mathbb{Z}[i]$ como un corolario de una ley de orden superior sin relacionarla con la ley para $\mathbb{Z}$. Fue Dirichlet quién demostró que esta ley para enteros gaussianos podía deducirse directamente del Teorema 1.6.1 sin necesidad de usar reciprocidad bicuadrática.

Formalmente, definimos el conjunto de los enteros gaussianos como un subconjunto de los números complejos, tomando como parte real y parte imaginaria números enteros exclusivamente.

$$\mathbb{Z}[i] = \{\, a+bi \mid a\ ,\ b \in \mathbb{Z}\,\}, \quad i = \sqrt{-1}$$

Es claro que $\mathbb{Z} \subset \mathbb{Z}[i] \subset \mathbb{C}$. Clarificaremos dos cuestiones básicas que destacan sobre las demás: por un lado, cuáles son las unidades del anillo en cuestión; por el otro, cuáles son sus elementos primos.

Proposición 2.0.1. *Las unidades del anillo $\mathbb{Z}[i]$ son precisamente las raíces cuartas de la unidad.*

$$\mathbb{Z}[i]^x = \{1, i, -1, -i\}$$

Demostración. Notar que un número $\alpha = a+ib \in \mathbb{Z}[i]$ es una unidad si y sólo si su norma es 1. Suponer que $\alpha \in \mathbb{Z}[i]$ es una unidad, $N(1) = N(uu^{-1}) = N(u)N(u^{-1}) = 1,$ luego $N(u) = 1$. Ahora suponer que $\alpha = a+ib \in \mathbb{Z}[i]$ con $N(\alpha) = a^2+b^2 = 1$. Dado que $a,b \in \mathbb{Z}$, solo hay cuatro posibles soluciones: $(a,b) = (\pm 1, 0)$ ó $(a,b) = (0, \pm 1)$. Estas cuatro soluciones conducen a las cuatro unidades $1, i, -1, -i$. □

2.1. Primos en $\mathbb{Z}[\mathbf{i}]$

Es un hecho conocido que $\mathbb{Z}[i]$ es un dominio euclídeo (D.E.). Dado que cada D.E. es un dominio de ideales principales (D.I.P), esto significa que $\mathbb{Z}[i]$ es un D.I.P. Además, en un D.I.P todo elemento irreducible es un elemento primo, por lo que todo elemento irreducible en $\mathbb{Z}[i]$ es primo. Hay tres tipos diferentes de números primos en $\mathbb{Z}[i]$ conocidos como primos gaussianos.

Lema 2.1.1. *Sea $\alpha = a+bi \in \mathbb{Z}[i]$ y $N(\alpha) = a^2+b^2$ un elemento primo en $\mathbb{Z}$, entonces $\alpha \mid N(\alpha)$ y además α es un elemento primo en $\mathbb{Z}[i]$.*

Demostración. Supongamos que $\alpha = \beta\gamma$ con $\beta, \gamma \in \mathbb{Z}[i]$. Entonces, $N(\alpha) = N(\beta\gamma) = N(\beta)N(\gamma)$. Dado que $N(\alpha)$ es primo por hipótesis, entonces o bien, $N(\beta) = 1$ o bien, $N(\gamma) = 1$, y así o bien, β o bien γ es una unidad en $\mathbb{Z}[i]$. Finalmente, α irreducible en $\mathbb{Z}[i]$, lo que significa que es primo en $\mathbb{Z}[i]$. □

Teorema 2.1.2. *Sea $p \in \mathbb{Z}$ un primo impar, entonces $p = a^2+b^2$ $(a,b \in \mathbb{Z})$ si y sólo si $p \equiv 1$* (mód 4).

Demostración. En primer lugar, veamos que si $p \in \mathbb{Z}$ es un primo tal que $p \equiv 3 \pmod 4$, entonces p no se puede escribir como la suma de dos cuadrados. En $\mathbb{Z}_4$, si $x \in \mathbb{Z}$ es par, entonces $x^2 \equiv 0 \pmod 4$. Si x es impar, entonces $x^2 \equiv 1 \pmod 4$. Esto significa que $a^2 + b^2 \equiv 0, 1, 2 \pmod 4$. De ahí se sigue que $a^2 + b^2 \not\equiv 3 \pmod 4$. Por tanto, $p \equiv 3 \pmod 4$ no se puede escribir como la suma de dos cuadrados. Ahora, supongamos que $p \in \mathbb{Z}$ es un primo impar tal que $p \equiv 1 \pmod 4$, esto significa que $p = 4k+1$ para un cierto $k \in \mathbb{Z}$. Aplicando el Corolario 1.3.4

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{2k} = 1$$

Así, existe $b \in \mathbb{Z}$ tal que $b^2 \equiv -1 \pmod p$, entonces $p \mid b^2 + 1$. Al factorizar $b^2 + 1$ en $\mathbb{Z}[i]$, esto significa que $p \mid (b+i)(b-i)$. Dado que $p > 1$, $p \nmid (b+i)$ y $p \nmid (b-i)$. Esto implica que p no es primo en $\mathbb{Z}[i]$ y es por tanto un elemento reducible en $\mathbb{Z}[i]$. Luego, $p = \alpha\beta$ con $\alpha, \beta \in \mathbb{Z}[i]$ ambos no unidades. Al tomar la norma de ambos lados, nos queda la ecuación

$$N(p) = p^2 = N(\alpha)N(\beta)$$

Como $N(\alpha)$ y $N(\beta)$ son ambos > 1, $p = N(\alpha)$ y $p = N(\beta)$. Dado que $\alpha \in \mathbb{Z}[i]$, entonces $\alpha = a + bi$ para $a, b \in \mathbb{Z}$. Por lo tanto $p = a^2 + b^2$ y p se puede escribir como la suma de dos cuadrados. □

Proposición 2.1.3. *Los primos del anillo $\mathbb{Z}[i]$ son (salvo asociados):*

1. $1 + i$
2. *los primos $p \in \mathbb{Z}$ con $p \equiv 3 \pmod 4$*
3. *los divisores $a + bi$, $a - bi$ de los primos $p \in \mathbb{Z} \subset \mathbb{Z}[i]$ con $p \equiv 1 \pmod 4$, con $a > |b| > 0$*

Demostración.

- Notar que $N(1+i) = 2$, como 2 es primo, por el Lema 2.1.1, $1+i$ es un primo gaussiano. Además, $2 = (1+i)(1-i)$ y $1+i$ y $1-i$ son asociados ya que $1 + i = i(1-i)$, con lo que podría decirse que $1+i$ (y sus asociados) son los únicos primos gaussianos pares.

- Supongamos, a modo de contradicción, que $p \equiv 3 \pmod 4$ no es un primo gaussiano. Es decir, p no es un elemento irreducible de $\mathbb{Z}[i]$, lo que implica que existen $\alpha, \beta \in \mathbb{Z}[i]$ con $p = \alpha\beta$ y $N(\alpha) > 1$ y $N(\beta) > 1$. Tomando normas se tiene $N(p) = N(\alpha\beta)$ lo que implica $p^2 = N(\alpha)N(\beta)$. Por tanto, $p = N(\alpha)$. Sea ahora $\alpha = a + bi$ donde $a, b \in Z$. Esto significa que $p = a^2 + b^2$ lo cual contradice el Teorema 2.1.2 ya que $p \equiv 3 \pmod 4$. Por tanto, p es un primo gaussiano. De hecho, se considera que p es un primo gaussiano impar.

- Sea p un primo en $\mathbb{Z}$ tal que $p \equiv 1 \pmod 4$. Por el Teorema 2.1.2, esto significa que $p = a^2 + b^2$ con $a, b \in \mathbb{Z}$, o alternativamente, $p = (a+bi)(a-bi)$. Dado que $N(a+bi) = p$ y $N(a-bi) = p$, por el Lema 2.1.1, ambos son primos gaussianos. Razonemos por reducción al absurdo que son distintos (i.e no asociados). Supongamos que $a + bi$, $a - bi \in \mathbb{Z}[i]$ son asociados, es decir, existe u unidad en $\mathbb{Z}[i]$ tal que $u(a+bi) = a - bi$ (recordar que $u \in \{1, -1, i, -i\}$).

$$\begin{cases} a + ib = a - ib \implies 2b = 0 \implies p = a^2 & \implies \quad a \mid p \\ -a - ib = a - ib \implies 2a = 0 \implies p = b^2 & \implies \quad b \mid p \\ -b + ai = a - ib \implies a = -b \implies p = 2a^2 & \implies \quad 2 \mid p \\ b - ai = a - ib \implies a = b \implies p = 2a^2 & \implies \quad 2 \mid p \end{cases}$$

  Analizaremos con más detalle el primer caso (el resto de casos son análogos).

Como $p \in \mathbb{Z}$ es primo impar, o bien $a = \pm 1$ o bien $a = \pm p$.

$$\begin{cases} \text{Si } a = \pm 1 \implies & p = 1 \\ \text{Si } a = \pm p \implies & p = p^2 \implies p(1-p) = 0 \implies p = 0 \text{ ó } p = 1 \end{cases}$$

En todos estos supuestos se llega a una contradicción con $p \in \mathbb{Z}$ primo impar. Por tanto, $a+ib$ y $a-ib$ no son asociados, por lo que son primos gaussianos distintos.

Por último, tenemos que comprobar que un elemento primo arbitrario π de $\mathbb{Z}[i]$ está asociado a uno de los casos anteriores. Notar que la descomposición $N(\pi) = \pi\overline{\pi} = p_1 \dots p_r$ con primos p_i, muestra que $\pi \mid p$ para algún $p = p_i$. Esto nos dice que $N(\pi) \mid N(p) = p^2$, luego, o bien $N(\pi) = p$, o bien, $N(\pi) = p^2$.

- Si $N(\pi) = p$, $\pi = a+bi$ con $a^2+b^2 = p$, π es del tipo 3 o del tipo 1 si $p = 2$.
- Si $N(\pi) = p^2$, entonces π está asociado a p ya que $p \mid \pi$ es un entero con norma uno y por tanto, una unidad. Así π es del tipo 2 (si no fuese así tendríamos $p = 2$ o $p = 1 \pmod 4$ y debido al Teorema 2.1.2 $p = a^2+b^2 = (a+bi)(a-bi)$ no podría ser primo).

□

En efecto, hemos visto que para encontrar todos los números primos en $\mathbb{Z}[i]$, solo necesitábamos fijarnos en los primos impares (mód 4) en $\mathbb{Z}$ y sus factores en $\mathbb{Z}[i]$ (con la salvedad de $2 \in \mathbb{Z}$ y su factor doble en $\mathbb{Z}[i]$). Por supuesto, los primos en $\mathbb{Z}$ no son necesariamente primos en $\mathbb{Z}[i]$ como acabamos de demostrar. Por ejemplo, para $p = 5 \in \mathbb{Z}$ se tiene $5 = (1+2i)(1-2i)$, luego 5 no es primo en $\mathbb{Z}[i]$ pero sus divisores son del tipo 2 y entonces son primos gaussianos. Nos interesará en este punto saber cómo referirnos a los primos de $\mathbb{Z}$ que siguen siendo primos en $\mathbb{Z}[i]$.

1. Si $p = 2 \in \mathbb{Z}$, p factoriza en el producto de una unidad por un cuadrado en $\mathbb{Z}[i]$, $2 = -i(1+i)^2$ y se dice *ramificado*.
2. Si $p \in \mathbb{Z}$ con $p \equiv 3 \pmod 4$, p sigue siendo primo en la extensión $\mathbb{Z}[i]$ de $\mathbb{Z}$ y se dice *inerte*.
3. Si $p \in \mathbb{Z}$ con $p \equiv 1 \pmod 4$, p factoriza en el producto de dos elementos distintos de $\mathbb{Z}[i]$, es decir, $p = (a+ib)(a-ib)$ y se dice que está *totalmente dividido* en $\mathbb{Z}[i]$.

2.2. Anillo cociente $\mathbb{Z}[\mathbf{i}]/(\pi)$

Dados $a,b,c,d \in \mathbb{Z}$, $\pi \in \mathbb{Z}[i]$, podemos definir clases de residuos en $\mathbb{Z}[i]$.

$$a+bi \equiv c+di \pmod{\pi} \quad \text{si} \quad \pi \mid (\,(a-c)+(b-d)i\,)$$

1. Sea $\pi = 1+i$. En particular, $i \equiv -1 \pmod{\pi}$, luego $a+bi \equiv a-b \pmod{\pi}$. Además, $\pi \mid 2$ y podemos reducir $a-b \pmod 2$. Luego, $\mathbb{Z}[i]/(\pi) = \{0,1\}$ y hay 2 clases de residuos (mód π) .
2. Sea $\pi = p$ con $p \equiv 3 \pmod 4$ ($p \in \mathbb{Z}$). En particular, $\pi \mid p$ y podemos reducir $a,b \pmod p$. Nos gustaría que $\mathbb{Z}[i]/(\pi)$ fuese $\{a+bi \mid 0 \le a,b < p\}$, es decir, un conjunto con p^2 elementos. Como $\pi \mid p$, tenemos que $a+bi \equiv c+di \pmod{\pi}$ para algún $a+bi \in \mathbb{Z}[i]/(\pi)$. Sólo falta demostrar que no existen dos elementos en $\mathbb{Z}[i]/(\pi)$ que sean congruentes (mód π). Supongamos que $a+bi \equiv c+di \pmod{\pi}$ para $0 \le a,b < p$. Entonces $\pi = p \mid (\,(a-c)+(b-d)i\,)$, es decir, $\frac{a-c}{p} + \frac{b-d}{p}i \in \mathbb{Z}[i]$. Esto sucede si y sólo si $a \equiv c \pmod p$ y $b \equiv d \pmod p$, lo que implica $a = c$ y $b = d$. Estábamos en lo cierto, $\mathbb{Z}[i]/(\pi) = \{a+bi \mid 0 \le a,b < p\}$ y hay p^2 clases de residuos (mód π).

3. Sea $\pi = a+bi$ con $N(\pi) = p \equiv 1 \pmod 4$ ($p \in \mathbb{Z}$). En particular, elegiendo $c+di \in \mathbb{Z}[i]$, $i \equiv -\frac{c}{d} \pmod \pi$, luego $a+bi \equiv a-b\frac{c}{d} \pmod \pi$. Además, $\pi \mid p$ y podemos reducir $a-b\frac{c}{d} \pmod p$. Nos gustaría que $\mathbb{Z}[i]/(\pi)$ fuese $\{0,1\dots p-1\}$, es decir, un conjunto con p elementos. En efecto, sólo falta demostrar que no existen dos elementos en $\mathbb{Z}[i]/(\pi)$ que sean congruentes (mód π). Si $a \equiv c \pmod \pi$ con $0 \le a,c < p$, entonces $\pi \mid (a-c)$, tomando normas $N(\pi) = p \mid (a-c)^2$, luego $p \mid (a-c)$ y $a = c$. Finalmente, $\mathbb{Z}[i]/(\pi) = \{0,1\dots p-1\}$ y hay p clases de residuos (mód π).

Teorema 2.2.1. *Si π es primo en $\mathbb{Z}[i]$, entonces $\mathbb{Z}[i]/(\pi)$ es un cuerpo finito con $N(\pi)$ elementos.*

Demostración.

- Si $\pi = 1+i$, acabamos de probar que $\mathbb{Z}[i]/(\pi) = \{0,1\}$ y es claro que forma cuerpo finito con $N(1+i) = 2$ elementos.
- Si $\pi = p$ con $p \equiv 3 \pmod 4$ ($p \in \mathbb{Z}$), veamos que $\mathbb{Z}[i]/(\pi)$ es un dominio, es decir, que no tiene divisores cero. De hecho, supongamos que $(a+bi)(c+di) \equiv 0 \pmod \pi$. Como π es primo en $\mathbb{Z}[i]$, $\pi \mid (a+bi)$ o $\pi \mid (c+di)$, por lo tanto $[a+bi]_\pi = [0]_\pi$ o $[c+di]_\pi = [0]_\pi$. Esto muestra que efectivamente es un dominio y es conocido que todo dominio con un número finito de elementos es cuerpo. En particular, $Z[i]/(\pi)$ es un cuerpo con $N(\pi) = p^2$ elementos.
- Si $\pi = a+bi$ con $N(\pi) = p \equiv 1 \pmod 4$ ($p \in \mathbb{Z}$), definamos la aplicación $\lambda : \mathbb{Z}/(p) \to \mathbb{Z}[i]/(\pi) : [r]_p \mapsto [r]_\pi$. Esta aplicación es claramente un homomorfismo (isomorfismo) porque $\lambda([r]_p)\lambda([s]_p) = [r]_\pi[s]_\pi = [rs]_\pi = \lambda([rs]_p)$. Además, es suprayectivo porque cada clase de residuo módulo π está representado por uno de los números enteros $0,1,\dots,p-1$. También inyectivo, en efecto, $Ker\lambda = \{[r]_p \mid [r]_\pi = [0]_\pi\}$ y si $r \equiv 0 \pmod \pi$, entonces $p^2 \mid r^2$, por tanto, $p \mid r$, $[r]_p = [0]_p$ y $Ker\lambda = [0]_p$. Por ser isomorfismo, los dos anillos de restos tienen el mismo número de elementos, la misma estructura, y en particular, ambos son cuerpos finitos con $N(\pi) = p$ elementos.

□

2.3. La ley de reciprocidad cuadrática

Llegados a este punto, uno podría ya intuir la analogía que se tiene entre $\mathbb{Z}_p$ y $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$. Uno de los resultados esperable podría ser un resultado análogo al pequeño Teorema de Fermat para $\mathbb{Z}$, también un análogo para el criterio de Euler (1.3.1) y una especie de símbolo de Legendre gaussiano.

Teorema 2.3.1 (Teorema de Fermat)**.** *Dado $\alpha \in (Z[i]/\pi\mathbb{Z}[i])^{\,x}$ con $\pi = a+bi$ primo gaussiano impar,*

$$\alpha^{N(\pi)-1} \equiv 1 \pmod \pi$$

Demostración. No daremos una demostración formal por su similitud con la de $\mathbb{Z}$, recordar 1.2. □

Lema 2.3.2 (Criterio de Euler)**.** *Sea π un primo gaussiano impar, entonces:*

$$\alpha^{\frac{N(\pi)-1}{2}} \equiv \pm 1 \pmod \pi$$

Demostración. $\pi = a+bi \equiv 1 \pmod 2$ por ser primo gaussiano impar, $N(\pi) = a^2+b^2 \equiv 1 \pmod 4$.

$$\alpha^{N(\pi)-1} - 1 = \left(\alpha^{\frac{N(\pi)-1}{2}} - 1\right)\left(\alpha^{\frac{N(\pi)-1}{2}} + 1\right) \equiv 0 \pmod \pi, \quad \alpha^{\frac{N(\pi)-1}{2}} \equiv \pm 1 \pmod \pi$$

□

Definición 2.3.3. El símbolo de Legendre gaussiano viene dado por:

$$\left[\frac{\alpha}{\pi}\right] := \begin{cases} 1 & \text{si existe } \eta \in \mathbb{Z}[i] \text{ tal que } \eta^2 \equiv \alpha \pmod{\pi} \\ -1 & \text{en otro caso} \end{cases}$$

Proposición 2.3.4. *Si* $\alpha, \beta \in (Z[i]/\pi\mathbb{Z}[i])^{\times}$, $\pi = a+bi \equiv 1 \pmod 2$, *se tiene:*

- $\left[\frac{\alpha}{\pi}\right] = \left[\frac{\beta}{\pi}\right]$ *si* $\alpha \equiv \beta \pmod{\pi}$
- $\left[\frac{\alpha\beta}{\pi}\right] = \left[\frac{\alpha}{\pi}\right]\left[\frac{\beta}{\pi}\right]$

Demostración. Análogas a las de $\mathbb{Z}$, véase por ejemplo 1.2.3. □

Observación 2.3.5. Es importante señalar que el símbolo de Legendre gaussiano no siempre coincide con el símbolo de Legendre usual, por ejemplo, $\left(\frac{2}{3}\right) = -1$ y $\left[\frac{2}{3}\right] = 1 \neq -1$ ya que $i^2 = -1 \equiv 2 \pmod 3$.

Teorema 2.3.6. *Sean* $\lambda = a+bi$, $\mu = c+di \in \mathbb{Z}[i]$ *dos primos gaussianos impares y distintos, entonces:*

$$\left[\frac{\lambda}{\mu}\right] = \left[\frac{\mu}{\lambda}\right]$$

Demostración. Véase [8, Prop. 5.1, p. 154 y sig.] □

Corolario 2.3.7. *Sean* $\pi = a+bi \in \mathbb{Z}[i]$ *un primo gaussiano impar, entonces se verifica:*

$$\left[\frac{i}{\pi}\right] = (-1)^{\frac{b}{2}}, \qquad \left[\frac{1+i}{\pi}\right] = \left(\frac{2}{a+b}\right)$$

Demostración. Véase [8, Prop. 5.1, p. 154 y sig.] □

Ejemplo 2.3.8. Por último, recordar que terminábamos el Capítulo con el Ejemplo 1.6.3. Extender esto a elementos $\alpha \in \mathbb{Z}[i]$ es posible pero se le debe exigir una condición bastante fuerte y es que sea D.F.U. que en particular es cierto por ser D.I.P. Así, un elemento cualquiera α del anillo de enteros gaussianos puede escribirse como $\alpha = i^k(1+i)^{k_0}\gamma_1^{k_1}\dots\gamma_s^{k_s}$, $k_0 = 0,1$ y se sigue:

$$\left[\frac{\alpha}{\pi}\right] = \left[\frac{i}{\pi}\right]^k \left[\frac{1+i}{\pi}\right]^{k_0} \left[\frac{\gamma_1}{\pi}\right]^{k_1} \dots \left[\frac{\gamma_s}{\pi}\right]^{k_s}$$

No conformes con enunciar la ley de reciprocidad cuadrática en el anillo de enteros gaussianos, buscaremos en el próximo capítulo enunciarla en uno más general, a saber, el de los enteros cuadráticos. Antes, daremos una proposición que los conecte.

Proposición 2.3.9. $\mathbb{Z}[i]$ *está compuesto por los elementos de la extensión* $\mathbb{Q}(i)$ *de* $\mathbb{Q}$ *que son raíces para un cierto polinomio mónico* $x^2+ax+b = 0$ *con coeficientes* $a, b \in \mathbb{Z}$.

Demostración. Sea $\alpha = c+di \in \mathbb{Q}(i)$ una raíz del polinomio $x^2+ax+b \in \mathbb{Q}[x]$ y suponer que $c,d \in \mathbb{Z}$. Notar que $(c+di)^2 + a(c+di) + b = (b+ac+c^2+d^2) + (2cd+ad)i = 0$, así $a = -2c, b = c^2+d^2$. Como c y d son enteros, necesariamente lo son a y b. Ahora bien, suponer que a y b son enteros, también lo son $2c$ y $2d$. De $(2c)^2 + (2d)^2 = 4b \equiv 0 \pmod 4$, se sigue que $(2c)^2 \equiv (2d)^2 \equiv 0 \pmod 4$, ya que los cuadrados $(\text{mód } 4)$ son siempre $\equiv 0, 1$, luego c y d enteros. □

Capítulo 3

La ley de reciprocidad cuadrática aplicada a $\mathscr{O}_K$

En este capítulo, consideraremos extensiones cuadráticas de $\mathbb{Q}$, es decir, extensiones de cuerpos $K/\mathbb{Q}$ de grado 2. Dentro de cada cuerpo K definiremos su anillo de enteros $\mathscr{O}_K$. Los anillos $\mathscr{O}_K$ conservan algunas propiedades de $\mathbb{Z}$, como por ejemplo que todo ideal se factoriza de manera única (salvo orden) como producto de ideales primos. Sin embargo, $\mathscr{O}_K$ no necesariamente es un dominio de ideales principales, por lo que no se asegura la factorización única de elementos.

3.1. Cuerpos cuadráticos

Recordar que dada una extensión $K/\mathbb{Q}$ sobre los racionales, se dice que un elemento $\alpha \in K/\mathbb{Q}$ es un entero algebraico si es raíz de un polinomio mónico no nulo con coeficientes enteros. Asimismo, se entiende por cuerpo de números algebraicos cualquier extensión de cuerpos finita de $\mathbb{Q}$. En particular, llamaremos cuerpo cuadrático a una extensión de cuerpos $K/\mathbb{Q}$ de grado 2. Si $K/\mathbb{Q}$ es una extensión de cuerpos con $[K:\mathbb{Q}] = 2$ y α un elemento de K que no está contenido en $\mathbb{Q}$, sabemos que α debe satisfacer una ecuación de grado 2 (no puede ser de grado 1 porque $\alpha \notin \mathbb{Q}$). Es más, sabemos que el polinomio mínimo de α es $p(x) = x^2 + bx + c \in \mathbb{Q}[X]$. Como $\mathbb{Q} \subset (\mathbb{Q}(\alpha)) \subset K$ y $\mathbb{Q}(\alpha)$ es un espacio vectorial sobre $\mathbb{Q}$ de dimensión 2, se sigue $K = \mathbb{Q}(\alpha)$. Por otro lado, completando cuadrados se obtiene $p(x) = \left(x + \frac{b}{2}\right)^2 - \frac{b^2-4c}{4}$. Como $\alpha \notin \mathbb{Q}$, $b^2 - 4c$ no es un cuadrado en $\mathbb{Q}$, y podemos tomar $D^2 = b^2 - 4c \in K$. En particular, $D = \sqrt{b^2-4c}$ denota una raíz de la ecuación $x^2 - (b^2 - 4c) = 0 \in K$. Afirmamos que $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{D})$. Como $\alpha \in \mathbb{Q}(\sqrt{D}), \mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt{D})$. Recíprocamente, $D = 2\alpha + b \in \mathbb{Q}(\alpha)$, de donde se deduce que $\mathbb{Q}(\sqrt{D}) \subset \mathbb{Q}(\alpha)$ y finalmente $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{D})$.

Si no aclaramos lo contrario, cuando escribamos $\mathbb{Q}(\sqrt{D})$ estaremos asumiendo que D es un entero libre de cuadrados, esto es, D no es divisible por ningún cuadrado perfecto distinto de 1, o dicho de otro modo, D es el producto de primos distintos. Esto no supone una pérdida de la generalidad ya que si $D_1 = k^2 D_2$ para un cierto $k \in \mathbb{Q}$, entonces $a + b\sqrt{D_2} = a + bk\sqrt{D_1}$ y así $\mathbb{Q}(\sqrt{D_1}) = \mathbb{Q}(\sqrt{D_2})$.

Observación 3.1.1. $x^2 \equiv D \pmod{p}$ es resoluble si y sólo si $\left(\frac{D}{p}\right) = 1$.

Proposición 3.1.2. *Todos los cuerpos cuadráticos son de la forma*

$$\mathbb{Q}(\sqrt{D}) = \mathbb{Q} + \mathbb{Q}\sqrt{D}$$

donde D es un (único) entero libre de cuadrados. Más aún, todos ellos son no isomorfos dos a dos.

Demostración. Ya visto con el razonamiento anterior. □

La aplicación $\mathscr{D} \mapsto \mathbb{Q}(\sqrt{D})$ es un biyección desde el conjunto de todos los enteros libres de cuadrados $D \neq \{0,1\}$ al conjunto de todos los cuerpos cuadráticos. Si $K = \mathbb{Q}(\sqrt{D})$ es un cuerpo cuadrático, entonces los dos $\mathbb{Q}$-homomorfismos de K en $\mathbb{C}$, son precisamente $\sigma_1(\alpha) = \alpha$ y $\sigma_2(\overline{\alpha}) = \overline{\alpha}$, donde $\overline{\alpha}$ denota el conjugado de α, es decir, para $\alpha = a + b\sqrt{D} \in K$, $\overline{\alpha} = a - \sqrt{D}$. Las aplicaciones $Tr : \mathbb{Q}[\sqrt{D}] \to \mathbb{Q}$ y $N : \mathbb{Q}[\sqrt{D}]^{\,x} \to \mathbb{Q}^{\,x}$ son homomorfismos de grupos aditivos y multiplicativos, respectivamente.

- $Tr_K(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) = \alpha + \overline{\alpha} = (a + b\sqrt{D}) + (a - b\sqrt{D}) = 2a$
- $N_K(\alpha) = \sigma_1(\alpha)\sigma_2(\alpha) = \alpha\overline{\alpha} = (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2$

Dado un polinomio mónico de segundo grado $p(x) \in \mathbb{Q}[x]$ que satisface $p(\alpha) = 0$, también $p(\overline{\alpha}) = 0$, por lo que $(x - \alpha) \mid p(x)$ y así $(x - \overline{\alpha}) \mid p(x)$, de donde se sigue:

$$p(x) = (x - \alpha)(x - \overline{\alpha}) = x^2 + (\alpha + \overline{\alpha})x - \alpha\overline{\alpha} = x^2 + Tr(\alpha)x - N(\alpha)$$

Es más, el polinomio mínimo de α sobre $\mathbb{Q}$ es precisamente $p(x)$ como demostraremos a continuación.

Proposición 3.1.3. *Sea α un entero algebraico y $f(x)$ un polinomio mónico en $\mathbb{Z}[x]$ de grado mínimo que tiene a α como raíz. Entonces $f(x)$ es irreducible en $\mathbb{Q}[x]$ y es el polinomio mínimo de α sobre $\mathbb{Q}$.*

Demostración. Supongamos que $f(x)$ no es irreducible en $\mathbb{Q}[x]$, esto es, $\exists g(x), h(x) \in \mathbb{Q}[x]$ con grado$(g(x))$, grado$(h(x)) > 0$, tal que $f(x) = g(x)h(x)$. Sea $n \in \mathbb{Z}$ el menor entero positivo tal que $ng(x) \in Z[x]$ y m el menor entero positivo tal que $mh(x) \in \mathbb{Z}[x]$. La minimalidad de n y m nos aseguran que $ng(x)$ y $mh(x)$ son primitivos. Si $nm > 1$ y p es cualquier primo divisor de nm, al reducir coeficientes módulo p en la ecuación $nmf(x) = (ng(x))(mh(x))$, tenemos que $0 = (ng(x))(mh(x))$ en $\mathbb{Z}_p[x]$. Como $\mathbb{Z}_p[x]$ es un dominio de integridad, debe ser $ng(x) = 0$ o $mh(x) = 0$. Por ello, p divide a todos los coeficientes de $ng(x)$ o a todos los coeficientes de $mh(x)$, pero esto es imposible ya que $ng(x)$ y $mh(x)$ son primitivos. Por lo tanto, ha de ser $n = m = 1$ y $g(x), h(x) \in \mathbb{Z}[x]$. Como α es raíz de alguno de los dos polinomios anteriores y ambos tienen grado menor que $f(x)$, se llega a una contradicción. □

Observación 3.1.4. Para que α sea un entero algebraico, no se requiere que el polinomio $f(x)$ sea irreducible en $\mathbb{Q}[x]$. Sin embargo, sí es cierto que cada entero algebraico α es raíz de algún polinomio mónico con coeficientes enteros e irreducible en $\mathbb{Q}[x]$.

3.2. Anillo de enteros cuadráticos $\mathscr{O}_K$

Se dice que $\alpha \in K/\mathbb{Q}$ es un entero cuadrático del cuerpo cuadrático $K = \mathbb{Q}(\sqrt{D})$ si $p(x) \in \mathbb{Z}[\alpha]$ y esto sucede si y sólo si $Tr_K(\alpha) = 2a \in \mathbb{Z}$ y $N_K(\alpha) = a^2 - Db^2 \in \mathbb{Z}$. Si $K/\mathbb{Q}$ es un cuerpo de números cuadráticos, los enteros cuadráticos contenidos en K forman un anillo, comúnmente denotado $\mathscr{O}_K$.

$$\mathscr{O}_K = \{\ \alpha \in K \mid \exists\ 0 \neq f(x) \in \mathbb{Z}[X] \quad \text{t.q} \quad f(\alpha) = 0\ \}$$

Los anillos de enteros cuadráticos $\mathscr{O}_K$, presentan ciertas propiedades de $\mathbb{Z}$, como por ejemplo que todo elemento no nulo ni unidad se factoriza como producto de irreducibles. Es más, si K es un cuerpo cuadrático, se tiene que $\mathscr{O}_K$ es DFU. A menos que señaleremos lo contrario, $K = \mathbb{Q}(\sqrt{D})$.

Proposición 3.2.1. *Sea $K = \mathbb{Q}(\sqrt{D})$, entonces $\mathscr{O}_K = \mathbb{Z} + \mathbb{Z}\alpha = \mathbb{Z}[\alpha]$ donde*

$$\alpha = \begin{cases} \sqrt{D} & \text{si } D \equiv 2,3 \pmod 4 \\ \frac{1+\sqrt{D}}{2} & \text{si } D \equiv 1 \pmod 4 \end{cases}$$

Demostración. Notar que α está en $\mathscr{O}_K$ tanto si $D \equiv 2,3 \pmod 4$ como si $D \equiv 1 \pmod 4$, ya que α satisface una ecuación mónica en $\mathbb{Z}[X]$ en ambos casos, $X^2 - D = 0$ y $X^2 - X + \frac{1-D}{4}$ respectivamente. En efecto, si $D \not\equiv 1 \pmod 4$, $\alpha^2 - D = 0$. Análogamente, si $D \equiv 1 \pmod 4$, se tiene $(2\alpha - 1)^2 = D$, así $4\alpha^2 - 4\alpha + 1 - D = 0$ y entonces $\alpha^2 - \alpha + \frac{1-D}{4}$. Con lo que se concluye que $\mathbb{Z} + \mathbb{Z}\alpha \subset \mathscr{O}_K$. Veamos

ahora que $\mathscr{O}_K \subset \mathbb{Z}+\mathbb{Z}\alpha$. Tomemos $\alpha = a+b\sqrt{D} \in \mathscr{O}_K$, así, $Tr_K(\alpha) = 2a \in \mathbb{Z}$ y $N_K(\alpha) = a^2 - Db^2 \in \mathbb{Z}$. Sean ahora $a = \frac{r}{2}$ y $b = \frac{m}{n}$ para algunos $m,n,r \in \mathbb{Z}$ con $(m.n) = 1$. Entonces $4m^2D = n^2(r^2 - 4N(\alpha))$, así $n^2 \mid 4m^2D$, y de hecho $n^2 \mid 4D$ porque $(m,n) = 1$. Si p fuese un primo impar tal que $p \mid n$, tendríamos que $p \mid D^2$, contradiciendo que D es libre de cuadrados. Así que tiene que ser una potencia de 2. Puesto que 4 no divide a D, $n^2 \mid 4D$, entonces $n^2 \mid 8$, por lo tanto, o bien, $n = 1$ o bien, $n = 2$, en ambos casos $b = \frac{s}{2}$, para algún $s \in \mathbb{Z}$. De $N_K(\alpha) = a^2 - Db^2 \in \mathbb{Z}$, tenemos que $r^2 \equiv s^2D \pmod 4$

- Si $D \not\equiv 1 \pmod 4$, $r^2 \equiv s^2 \equiv 0 \pmod 4$, y entonces r,s enteros pares con $a,b \in \mathbb{Z}$ y $\mathscr{O}_K \subset \mathbb{Z}+\mathbb{Z}\alpha$.
- Si $D \equiv 1 \pmod 4$, $r^2 \equiv s^2 \pmod 4$, y entonces r,s elementos de la misma paridad ($r \equiv s \pmod 2$). Escribiendo $r = s+2k$, $k \in \mathbb{Z}$, vemos que

$$\alpha = a+b\sqrt{D} = \frac{r+s\sqrt{D}}{2} = \frac{s+2k+s\sqrt{D}}{2} = k+s\frac{1+\sqrt{D}}{2}$$

Así $\mathscr{O}_K \subset \mathbb{Z}+\mathbb{Z}\frac{1+\alpha}{2}$.

□

Corolario 3.2.2. *El anillo de enteros cuadráticos $\mathscr{O}_K \cong \mathbb{Z}[X]/(f(X))$ donde*

$$f(X) = \begin{cases} X^2 - D & si\ D \not\equiv 1 \pmod 4 \\ X^2 - X + \frac{1-D}{4} & si\ D \equiv 1 \pmod 4 \end{cases}$$

(De hecho $f(X)$ es el polinomio irreducible de α sobre $\mathbb{Q}$).

Demostración. Por la proposición anterior, $\mathscr{O}_k = \mathbb{Z}[\alpha]$. Sea ahora $\varphi : \mathbb{Z}[X] \to \mathbb{Z}[\alpha]$ un homomorfismo de anillos, dado por $f(x) \mapsto f(\alpha)$. En particular, φ es suprayectivo, pues se trata del homomorfismo evaluación. Tomando $\tilde{\varphi} : \mathbb{Z}[X]/Ker\varphi \to \mathbb{Z}[\alpha]$, como $Ker\varphi = \{f(x) \in \mathbb{Z}[x] \mid f(\alpha) = 0\}$, podemos aplicar el Primer Teorema de Isomorfía y concluir que $\mathscr{O}_K \cong \mathbb{Z}[X]/(f(X))$. □

Definición 3.2.3. Llamaremos discriminante de $\alpha \in \mathscr{O}_K$ al elemento $d = Tr_K(\alpha)^2 - 4N(\alpha)$.

$$d = \begin{cases} 4D & \text{si } D \equiv 2,3 \pmod 4 \\ D & \text{si } D \equiv 1 \pmod 4 \end{cases}$$

3.3. Factorización en $\mathscr{O}_K$

En el desarrollo de esta sección, se optará por poner el foco en cuerpos cuadráticos imaginarios. La razón principal es que son el único cuerpo numérico, a parte de $\mathbb{Q}$, con un número finito de unidades. En particular, $|\mathscr{O}_K^x| = 2,4,8$ dependiendo de si $D = -1$, $D = -3$ o $D \notin \{-1,-3\}$, respectivamente.

Proposición 3.3.1. *Dado $u \in \mathscr{O}_K$, u es una unidad si y sólo si $N(u) = \pm 1$.*

Demostración. Supongamos que u es una unidad, $N(1) = N(uu^{-1}) = N(u)N(u^{-1}) = 1, \quad N(u) = \pm 1$. Recíprocamente, si $\pm 1 = N(u) = uu'$, entonces $u^{-1} = \pm u' \in \mathscr{O}_K$. □

Observación 3.3.2. (Norma de un elemento)

$$N(u) = \begin{cases} N(a+b\sqrt{D}) = a^2 - Db^2 & \text{si } D \not\equiv 1 \pmod 4 \text{ con } a,b \in \mathbb{Z}. \\ N(\frac{a+b\sqrt{D}}{2}) = \frac{a^2-Db^2}{4} & \text{si } D \equiv 1 \pmod 4 \text{ con } a \equiv b \pmod 2. \end{cases}$$

Ejemplo 3.3.3. (Unidades de cuerpos cuadráticos según el signo de D)

1. Si $K = \mathbb{Q}(\sqrt{D})$ $(D < 0)$
   - Si $D = -1$, $\mathscr{O}_K^{\,x} = Z[i]^{\,x} = \{\pm 1, \pm i\}$ (ya estudiado).
   - Si $D = -3$, $\mathscr{O}_K^{\,x} = Z[\frac{1+3i}{2}]^{\,x} = \{\pm 1, \pm\frac{1+3i}{2}, \pm\frac{1-3i}{2}\}$.
   - Si $D \notin \{-1,-3\}$, $\mathscr{O}_K^{\,x} = Z[\alpha]^{\,x} = \{\pm 1\}$.
2. Si $K = \mathbb{Q}(\sqrt{D})$ $(D > 0)$

   $a + b\sqrt{D}$ es una unidad en $\mathscr{O}_K$ si y sólo si (a,b) es solución de la ecuación $a^2 - Db^2 = \pm 1$

   A esta ecuación se le conoce como ecuación de Pell. Como D es un entero libre de cuadrados, existen infinitas soluciones de la ecuación de Pell (i.e. infinitas unidades en $\mathscr{O}_K$). En particular, si $u > 1$ es la menor unidad de $\mathscr{O}_K$, entonces $\mathscr{O}_K^{\,x} = \{ \pm u^n \mid n \in \mathbb{Z} \}$.

Es conocido que en un dominio de integridad, todo elemento primo es irreducible. Además, el recíproco es cierto en todo dominio de ideales principales, pero no lo es en general en $\mathscr{O}_K$ para un cuerpo K cualquiera. Para solventar esta problemática, introduciremos más adelante los ideales primos. No obstante, aquellos elementos de $\mathscr{O}_K$ cuya norma sea un primo, serán a su vez irreducibles.

Proposición 3.3.4. *Si $\gamma \in \mathscr{O}_K$ satisface $N(\gamma) = p$ con $p \in \mathbb{Z}$ primo, entonces γ es irreducible.*

Demostración. Supongamos que $\gamma \in \mathscr{O}_K$ es tal que $N(\gamma) = p$ con $p \in \mathbb{Z}$ primo. Si escribimos $\gamma = \alpha\beta$, entonces $p = N(\alpha)N(\beta)$, lo que implica que $N(\alpha) = \pm 1$ o $N(\beta) = \pm 1$, o equivalentemente α o β es una unidad y así, γ es irreducible. □

Teorema 3.3.5. *Todo $0 \neq \alpha \in \mathscr{O}_K$ no unidad se factoriza como producto de irreducibles en $\mathscr{O}_K$.*

Demostración. Si $\alpha \in \mathscr{O}_K$ no es nulo ni unidad, podemos suponer sin pérdida de generalidad que existe un divisor irreducible γ_1 para α, así $\alpha = \gamma_1\alpha_1$ con $1 \leq N(\alpha_1) < N(\alpha)$. Reiterando el proceso, si α_1 no es nulo ni unidad, entonces $\alpha_1 = \gamma_2\alpha_2$ (y $\alpha = \gamma_1\gamma_2\alpha_2$) con $1 \leq N(\alpha_2) < N(\alpha_1)$ y γ_2 irreducible, se obtiene así una sucesión decreciente de números naturales $N(\alpha), N(\alpha_1), N(\alpha_2), \ldots$ que eventualmente se estabilizará en 1, digamos $N(\alpha_j) = 1$. Por lo tanto, $\alpha = \gamma_1 \ldots \gamma_j\alpha_j$ elementos irreducibles. □

Este caso en el que un elemento de norma un número primo resulta irreducible representa una situación particular. Si se quieren resultados más generales, se tiene que optar por incluir ideales y buscar una factorización única de ideales. Analizado esto, es posible responder a qué primos $p \in \mathbb{Z}$ son de la forma $p = x^2 + Dy^2$, es decir, aquellos satisfaciendo $\left(\frac{d}{p}\right) = 1$ con d discriminante para K.

Proposición 3.3.6. *Sea $\mathfrak{a}$ un ideal no nulo en $\mathscr{O}_K$ donde K denota un cuerpo cuadrático, entonces $\mathfrak{a} \cap \mathbb{Z} = a\mathbb{Z}$ para algún $a \in \mathbb{Z}$. En particular, tomando $\mathfrak{p}$ un ideal primo no nulo de $\mathscr{O}_K$, $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$.*

Demostración.

- Sea $\mathfrak{a}$ un ideal no nulo en $\mathscr{O}_K$. Veamos que siempre contiene un entero no nulo. Sean $\alpha \in \mathfrak{a} \setminus 0$ y $f(x) = x^2 + bx + c \in \mathbb{Z}[x]$ su polinomio mínimo. Notar que $c \neq 0$ pues $f(x)$ es irreducible en $\mathbb{Q}[x]$. Como $f(\alpha) = 0$, tenemos $c = -\alpha(\alpha + b)$ por lo tanto $c \in \mathfrak{a} \cap \mathbb{Z}$. Además $\mathfrak{a} \cap \mathbb{Z}$ es un ideal de $\mathbb{Z}$, entonces $\mathfrak{a} \cap \mathbb{Z} = a\mathbb{Z}$ para algún $a \in \mathbb{Z}$.

- Sea ahora $\mathfrak{p}$ un ideal primo no nulo de $\mathscr{O}_K$. Veamos que $\mathfrak{p}$ contiene exactamente un primo $p \in \mathbb{Z}$. Si $a \in \mathfrak{p} \cap \mathbb{Z}$ y $a = p_1 \ldots p_k \in \mathbb{Z}$ es su descomposición en primos, entonces como $\mathfrak{p}$ es un ideal primo tenemos que $p_i \in \mathfrak{p}$ para algún i. Supongamos que p y q son dos primos distintos en $\mathfrak{p}$. Por ser coprimos existen $r, s \in \mathbb{Z}$ tales que $1 = pr + qs \in \mathfrak{p}$, por lo tanto $\mathscr{O}_K = \mathfrak{p}$, lo que contradice la hipótesis. Luego $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ para exactamente un primo $p \in \mathbb{Z}$.

□

Teorema 3.3.7. *Si $p \in \mathbb{Z}$ es un primo en $\mathbb{Z}$, $\tilde{f}(X) = f(X) + p\mathbb{Z}[X]$, $(p) = p\mathscr{O}_K$, entonces*

$$\mathscr{O}_K/p\mathscr{O}_K \cong \mathbb{Z}_p[X]/(\tilde{f}(X))$$

Demostración. Por el Corolario 3.2.2 se tiene $\mathscr{O}_K \cong \mathbb{Z}[X]/(f(X))$. También $p\mathscr{O}_K = (p) \cong (p, f(X))/(f(X))$. Así, basta aplicar dos veces el tercer teorema de isomorfía.

$$\mathscr{O}_K/p\mathscr{O}_K = (\mathbb{Z}[X]/(f(X)))/(p, f(X))/(f(X)) \cong \mathbb{Z}[X]/(p, f(X)) \cong$$
$$\cong (\mathbb{Z}[X]/(p))/(p, f(X))/(p) \cong \mathbb{Z}_p[X]/(\tilde{f}(X))$$

□

Corolario 3.3.8. *Sea el anillo cociente $\mathscr{O}_K/p\mathscr{O}_K \cong \mathbb{Z}_p[X]/(\tilde{f}(X))$ y $\left(\frac{d}{p}\right) = 1$, entonces:*

$$\tilde{f}(X) = \begin{cases} (X+a)(X-a) & \text{si } D \equiv 2,3 \pmod 4 \\ \left(X + \frac{1+\sqrt{a}}{2}\right)\left(X + \frac{1-\sqrt{a}}{2}\right) & \text{si } D \equiv 1 \pmod 4 \end{cases}$$

Demostración. Recordar que $d = 4D$ si $D \equiv 2,3 \pmod 4$ y $d = D$ si $D \equiv 1 \pmod 4$. Si $\left(\frac{d}{p}\right) = 1$, entonces $\exists\, a \neq 0$ en $\mathbb{Z}_p$ tal que $a^2 \equiv d \pmod p$ y basta sustituir notando que $\tilde{f}(X) = f(X) + p\mathbb{Z}[X]$ con $f(X)$ como en el Corolario 3.2.2. □

Por lo tanto, $p\mathscr{O}_K$ es primo, es decir, p es primo en $\mathscr{O}_K$ si y solo si $\mathbb{Z}_p[X]/(\tilde{f}(X))$ es un cuerpo (i.e, si $\tilde{f}(X)$ es irreducible) y eso sucede si y sólo si su discriminante d no es un cuadrado.

Proposición 3.3.9.

1. *Si $K/\mathbb{Q}$ es una extensión cuadrática y $p \in \mathbb{Z}$ un primo impar, se tiene:*
   - *p se ramifica en $\mathbb{Q}\sqrt{D}$ si $p\mathscr{O}_K = \mathfrak{p}^2$ para un ideal primo $\mathfrak{p}$ si y sólo si $\left(\frac{d}{p}\right) = 0$.*
   - *p está totalmente dividido en $\mathbb{Q}\sqrt{D}$ si $\mathfrak{p}_1\mathfrak{p}_2$ para ideales primos $\mathfrak{p}_1 \neq \mathfrak{p}_2$ si y sólo si $\left(\frac{d}{p}\right) = 1$.*
   - *p es inerte en $\mathbb{Q}\sqrt{D}$ si sigue siendo primo en $\mathscr{O}_K$ si y sólo si $\left(\frac{d}{p}\right) = -1$.*
2. *Si $K/\mathbb{Q}$ es una extensión cuadrática y $p = 2 \in \mathbb{Z}$ un primo par. En particular, se sigue:*
   - *$p = \mathfrak{p}^2$ se ramifica en $\mathbb{Q}\sqrt{D}$ si y sólo si $d \equiv 0,4 \pmod 8$.*
   - *$p = \mathfrak{p}_1\mathfrak{p}_2$ está totalmente dividido en $\mathbb{Q}\sqrt{D}$ si y sólo si $d \equiv 1 \pmod 8$*
   - *p es inerte en $\mathbb{Q}\sqrt{D}$ si y sólo si $d \equiv 5 \pmod 8$*

Demostración. Son comprobaciones al estilo de la demostración 3.3.8. □

Teorema 3.3.10. *Sea $K/\mathbb{Q}$ una extensión algebraica finita y supongamos que existe $\theta \in \mathscr{O}_K$ con $\mathscr{O}_K = \mathbb{Z}[\theta]$. Sea $p \in \mathbb{Z}$ un primo y sea $f(X) \in \mathbb{Z}[X]$ el polinomio irreducible de θ sobre $\mathbb{Q}$. Supongamos que $\tilde{f} \in \mathbb{F}_p[X]$ se descompone en la forma*

$$\tilde{f} = F_1^{e_1} \dots F_r^{e_r}$$

en $\mathbb{F}_p[X]$, con los $F_i \in p[X]$ irreducible para cada i. Sea $g_i \in \mathbb{Z}[X]$ un polinomio cumpliendo $\tilde{g}_i = F_i$ ($\pmod p$), entonces $\mathfrak{p}_i = (p, g_i(\theta))$ es primo en $\mathscr{O}_K$ y $p\mathscr{O}_K = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_r^{e_r}$

Demostración. Véase [9]. □

Ejemplo 3.3.11. (Anillo de enteros gaussianos) Ya hemos estudiado en profundidad lo que sucede en este anillo en el Capítulo 2. No obstante, lo reformularemos en términos de ideales.

Sea $K=\mathbb{Q}$ y $L=\mathbb{Q}(i)$. Dado que $\mathscr{O}_K=\mathbb{Z}$ es un D.I.P., cualquier ideal primo de $\mathscr{O}_K$ es de la forma (p) donde p es un primo de $\mathbb{Z}$. Si $p=x^2+y^2=N_{L/K}$ entonces $p=\mathfrak{p}_1\mathfrak{p}_2$ para algunos $\mathfrak{p}_1,\mathfrak{p}_2\in\mathscr{O}_L$ y $(p)=(\mathfrak{p}_1)(\mathfrak{p}_2)$ en $\mathscr{O}_L$, es decir, (p) es un producto de dos ideales principales en $\mathscr{O}_L$. Además $p_1=(\mathfrak{p}_1)$ y $p_2=(\mathfrak{p}_2)$ son primos ya que tienen la norma p. Los ideales p_1 y p_2 son distintos excepto en el caso $p=2=(1+i)(1-i)$ ya que $1+i=-i(1-i)$, es decir, $1+i$ y $1-i$ difieren en unidades. Si p no es una suma de dos cuadrados, esto significa que no hay ningún elemento de la norma p en $\mathscr{O}_L$, entonces p es irreducible en $\mathscr{O}_L$. Así $(p)=pOL=\{p\alpha \mid \alpha\in\mathscr{O}_L\}$ es en sí mismo un ideal primo. Por lo tanto, en este ejemplo, hay 3 posibilidades de lo que sucede con un $p\mathscr{O}_K$ ideal primo de K en la extensión L.

1. $(p)=p^2$ en $\mathscr{O}_L$ si $p=2$, es decir, se ramifica.
2. $(p)=p_1p_2$ en $\mathscr{O}_L$ si $p=x^2+y^2$, es decir, si $p\equiv 1 \pmod 4$ y se divide totalmente.
3. $(p)=p$ en $\mathscr{O}_L$ si $p=x^2+y^2$, es decir, si $p\equiv 3 \pmod 4$ y es inerte.

Ejemplo 3.3.12. La factorización de un primo impar p en $\mathbb{Q}(\sqrt{D})$ depende solamente del residuo $p \pmod{4D}$. Si $D=(-1)^j2^kp_1\dots p_r$, se sigue:

$$\left(\frac{d}{p}\right)=\left(\frac{-1}{p}\right)^j\left(\frac{2}{p}\right)^k\left(\frac{p_1}{p}\right)\dots\left(\frac{p_r}{p}\right)$$

3.4. La ley de reciprocidad cuadrática

Las ley vista en el Capítulo 2 es un caso especial de una ley más general que se aplica al anillo de números enteros en cualquier cuerpo numérico cuadrático imaginario. Aunque los detalles técnicos de las demostraciones de estos resultados escapan al objetivo de nuestro trabajo, por su interés, daremos la leyes de reciprocidad cuadráticas para el anillo de cuerpos cuadráticos y para el anillo de polinomios sobre un cuerpo finito.

Definición 3.4.1. Sea K un cuerpo cuadrático imaginario con un anillo de enteros $\mathscr{O}_K$. Para un ideal primo $\mathfrak{p}\subset\mathscr{O}_k$ con norma impar $\mathrm{N}(\mathfrak{p})$ y $\alpha\in\mathscr{O}_k$ se define el *carácter cuadrático* para $\mathscr{O}_k$ como

$$\left[\frac{\alpha}{\mathfrak{p}}\right]_2\equiv\alpha^{\frac{\mathrm{N}(\mathfrak{p})-1}{2}} \pmod{\mathfrak{p}}=\begin{cases}1 & \alpha\notin\mathfrak{p} \text{ and } \exists\eta\in\mathscr{O}_k \text{ tal que } \alpha-\eta^2\in\mathfrak{p}\\ -1 & \alpha\notin\mathfrak{p} \text{ y no existe tal } \eta\\ 0 & \alpha\in\mathfrak{p}\end{cases}$$

Proposición 3.4.2. *Dado $\mathfrak{a}\subset\mathscr{O}_k$ tal que $\mathfrak{a}=\mathfrak{p}_1\cdots\mathfrak{p}_n$ con $\mathfrak{p}_i$ primos y otro ideal $\beta\in\mathscr{O}_k$, se sigue:*

- $\left[\frac{\alpha}{\mathfrak{a}}\right]_2=\left[\frac{\alpha}{\mathfrak{p}_1}\right]_2\cdots\left[\frac{\alpha}{\mathfrak{p}_n}\right]_2$
- $\left[\frac{\alpha}{\beta}\right]_2=\left[\frac{\alpha}{\beta\mathscr{O}_k}\right]_2$

Demostración. Véase [8, Prop. 8.15, p. 256]. □

Teorema 3.4.3. *Sea $\mathscr{O}_k = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$, es decir, $\{\omega_1, \omega_2\}$ es una base integral para $\mathscr{O}_k$. Para $\nu \in \mathscr{O}_k$ con norma impar $\mathrm{N}(\nu)$, se toman $a,b,c,d \in \mathbb{Z}$ y una función $\chi : \mathscr{O}_k \to, \nu \mapsto \imath^{(b^2-a+2)c+(a^2-b+2)d+ad}$ tales que $\nu\omega_1 = a\omega_1 + b\omega_2$, $\nu\omega_2 = c\omega_1 + d\omega_2$. Si $m = \mathrm{N}(\mu)$ y $n = \mathrm{N}(\nu)$ son ambos impares, entonces:*

$$\left[\frac{\mu}{\nu}\right]_2 \left[\frac{\nu}{\mu}\right]_2 = (-1)^{\frac{m-1}{2}\frac{n-1}{2}} \chi(\mu)^{m\frac{n-1}{2}} \chi(\nu)^{-n\frac{m-1}{2}}$$

Demostración. Debida a Herglotz, puede consultarse en [8, Prop. 8.15, p. 256]. □

Anillo de polinomios sobre un cuerpo finito. Sea $\mathbb{F}$ un cuerpo finito con $q = p^n$ elementos, donde p es un número primo impar y n es positivo, y sea $\mathbb{F}[x]$ el anillo de polinomios en una variable con coeficientes en F.

Definición 3.4.4. Si $f,g \in \mathbb{F}[x]$ y f es irreducible, mónica y tiene grado positivo, se define el carácter cuadrático para $\mathbb{F}[x]$ de la manera habitual:

$$\left(\frac{g}{f}\right) = \begin{cases} 1 & (f,g) = 1 \text{ y } \exists h,k \in F[x] \text{ tal que } g - h^2 = kf \\ -1 & (f,g) = 1 \text{ y } g \text{ no es un cuadrado} \pmod{f} \\ 0 & (f,g) \neq 1 \end{cases}$$

Proposición 3.4.5. *Si $f = f_1 \cdots f_n$ es un producto de polinomios mónicos irreducibles*

$$\left(\frac{g}{f}\right) = \left(\frac{g}{f_1}\right) \cdots \left(\frac{g}{f_n}\right)$$

Demostración. Véase [1]. □

Teorema 3.4.6. *Si $f,g \in \mathbb{F}[x]$ son mónicos y de grado positivo*

$$\left(\frac{g}{f}\right)\left(\frac{f}{g}\right) = (-1)^{\frac{q-1}{2}(grado(f))(grado(g))}$$

Demostración. Debida a Dedekind, puede consultarse en [1, Thm. 6.7.16]. □

Bibliografía

[1] E. BACH, J. SHALLIT, *Algorithmic Number Theory (Vol I: Efficient Algorithms)*,The MIT Press. Cambridge,1996

[2] A. BAKER, *Breve introducción a la teoría de números*, Alianza Editorial, 1986

[3] P. M. COHN, *Algebra (Vol. I)*, Wiley & sons, 1974

[4] P. M. COHN, *Basic Algebra: Groups, rings and fields*, Springer, 2003

[5] K. IRELAND, M. ROSEN, *A Classical Introduction to Modern Number Theory* Springer, 1990

[6] N. JACOBSON, *Basic Algebra I*, Freeman and Co., 1980.

[7] A. KNOEBEL, R. LAUBENBACHER, J. LODDER, PENGELLEY, D. *Mathematical Masterpieces: Further Chronicles by the Explorers*[Patterns in Prime Numbers: The Quadratic Reciprocity Law], Springer, 2007

[8] F. LEMMERMEYER, *Reciprocity Laws: From Euler to Eisenstein*, Springer, 2000

[9] J. NEUKIRCH, *Algebraic Number Theory*, Springer, 1999

[10] J-P. SERRE, *A Course in Arithmetic*, Springer, 1978

[11] J. STILLWELL, *What Are Algebraic Integers and What Are They For?*, The American Mathematical Monthly, vol. 101, no. 3, 1994, pp. 266–270. JSTOR, `www.jstor.org/stable/2975607`

[12] A. WEIL, *Number theory: an approach through history from Hammurapi to Legendre*, Birkhäuser, 1987

Anexo I

Una demostración alternativa para la ley de reciprocidad cuadrática en $\mathbb{Z}$ (Teorema 1.6.1)

Sean p y q primos impares y distintos. Considérese un rectángulo R de vértices $(0,0)$, $(0,\frac{q}{2})$, $(\frac{p}{2},0)$ y $(\frac{p}{2},\frac{q}{2})$ y trázese su diagonal $qx-py=0$.

$$|R| = \#\left\{(x,y)\in\mathbb{R}^2 \;\mid\; 0<x\leq\frac{1}{2}(p-1)\;,\;\; 0<y\leq\frac{1}{2}(q-1)\right\} = \frac{1}{4}(p-1)(q-1)$$

Así, la LRC 1.6.1 es equivalente a

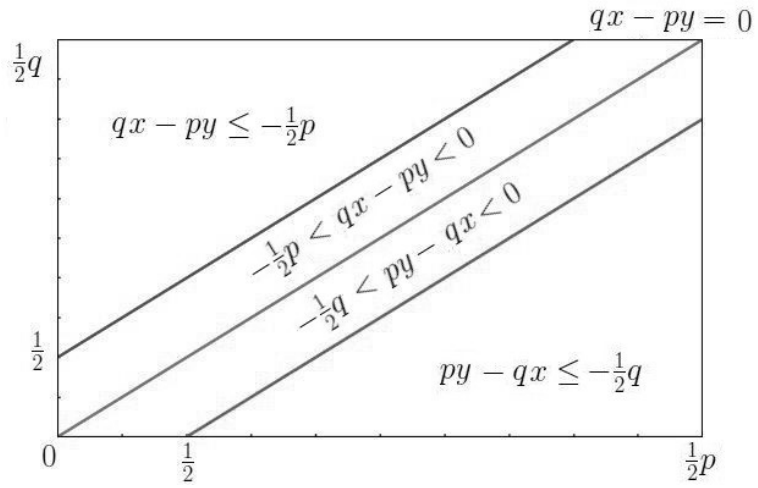
$$\left(\frac{q}{p}\right)\cdot\left(\frac{p}{q}\right) = (-1)^{|R|}$$

Por el Lema 1.5.1, $\left(\frac{q}{p}\right) = (-1)^l$, donde l es el número de elementos $x\in\{1,\ldots,\frac{1}{2}(p-1)\}$ para los cuales qx es negativo en p. Esta condición se satisface siempre que $py-\frac{1}{2}p<qx<py$. En efecto, notar que $\frac{q}{p}x<y<\frac{q}{p}x+\frac{1}{2}$. Como $0<x<\frac{p}{2}$, necesariamente $0<y<\frac{1}{2}(q+1)$. Ahora bien, $\frac{1}{2}(q+1)$ es el menor entero que sigue a $\frac{1}{2}(q-1)$ y se satisface $0<y<\frac{1}{2}(q-1)<\frac{1}{2}q$. Finalmente,

$$l = \#\left\{(x,y)\in R \;\mid\; -\frac{1}{2}p<qx-py<0\right\}$$

Intercambiando los papeles para p y q (y procediendo análogamente), $\left(\frac{q}{p}\right) = (-1)^m$, donde m es el número de elementos $y\in\{1,\ldots,\frac{1}{2}(q-1)\}$ para los cuales py es negativo en q.

$$m = \#\left\{(x,y)\in R \;\mid\; -\frac{1}{2}q<py-qx<0\right\}$$



Las regiones sobre las que contamos el número de puntos l y m son disjuntas como puede apreciarse en la figura superior.

$$\left(\frac{q}{p}\right)\cdot\left(\frac{p}{q}\right) = (-1)^{l+m}$$

Además, no hay puntos en $qx-py=0$ interiores a R (si existiese un punto tal, este sería un múltiplo positivo de pq, es decir, $x \geq \frac{pq}{q} = p \geq \frac{p}{2}$ y no pertenecería a R). Por simplicidad, denotaremos por A la región superior restante y B la región inferior restante.

$$A = \left\{ (x,y) \in R \ \mid \ qx - py \leq -\frac{1}{2}p \right\}, \quad B = \left\{ (x,y) \in R \ \mid \ py - qx \leq -\frac{1}{2}q \right\}$$

En estas dos regiones, puede comprobarse que el número de puntos es el mismo. Naturalmente, si $(x,y) \in R$, entonces para una cierta función ϕ satisfaciendo $\phi(x',y') \in R$ donde $x' = \frac{1}{2}(p+1) - x$, $y' = \frac{1}{2}(q+1) - y$ se tiene que $\phi^2 = \phi$ y así ϕ biyectiva.

Notar además que, dados $(x,y) \in R$, $(x,y) \in A$ si y sólo si $qx - py \leq -\frac{1}{2}p$ si y solo si $q\left(\frac{p+1}{2} - x'\right) - p\left(\frac{q+1}{2} - y'\right) \leq -\frac{1}{2}p$ si y solo si $py' - qx' \leq -\frac{1}{2}q$ si y solo si $(x',y') \in B$.

Así $\phi(A) = B$ y por ser ϕ biyectiva, $|A| = |B|$. Finalmente, $l + m = |R| - 2|A| \equiv |R| \pmod 2$.

$$\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{l+m} = (-1)^{|R|} = (-1)^{\frac{1}{4}(p-1)(q-1)}$$